Third International Seminar on Information Law 2010,

June 25-26 2010, Corfu Greece

Regulating speech on the Internet: myths, trends and realities

Panagiota Kelali
Associate Director
Center for Information Technology & Privacy Law
The John Marshall Law School
315 S. Plymouth Ct.
Chicago, Il 60604, USA
e-mail: 6kelali@jmls.edu

I. Introduction

In the early days of its existence, the "international network of interconnected computers"[1] was hailed as the "information superhighway"[2] and was viewed by many as the ultimate means to expand the freedom of speech worldwide.[3] As the court in ACLU v. Reno[4] explained, "it is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country - and indeed the world - has yet seen."[5] Indeed, users could become their own editors, disseminate information and give their opinions on a global scale. Free expression, distribution and reception of information never seemed so complete. For more than a decade, the Internet has been conceptualized as a forum for free expression with near limitless potential for individuals to express themselves and to access the expression of others holding the promise of an open platform for the exchange of ideas, accessibility, ease for mastery, and creativity. Internet was hailed as a place that knew no boundaries, where no sovereign ever reigned where anonymity and freedom of expression seemed to be safely guarded. However, reality turned out to be slightly different. The current proliferation of global information networks has prompted governments to regulate communication on these systems.[6]

As of December 31, 2009, Internet users were 1,802,330,457, an increase of 399% since 2000.[7] Undoubtedly the Internet has evolved to become the premier avenue of communication in the 21st century. There is no other medium where the single act of sharing information can raise issues of freedom of expression, privacy and intellectual property rights. When it comes to on-line speech, the simple reality is that the greater perceived ability for individuals and groups to communicate with each other and with the world at large using the Internet, the greater appears to be present day efforts to control such communications where governments perceive them to be politically undesirable. While there is no question that there are indeed certain types of speech or content which both governments and internet users would find harmful or undesirable and subject to control or even censorship, finding a commonly accepted definition and determination of what exactly that content is, constitutes an impossible feat.

Historically, legal efforts to censor or otherwise control internet "speech" have focused on the key players generally. Each of these has been the focus of varying attempts to censor speech, with varying degrees of success. This paper will examine the evolution of the attempts to regulate speech on the Internet, investigating the role of the key players, focusing on the regulatory solutions implemented by the US and the European Union and evaluating their efficacy. We will also examine the current status of Internet censorship globally as well as the trends for the future especially in view of the increasing concerns over national security, and the loss of economic value to content industries, pushing more countries for legislation to not only control content on the internet, but to enhance the technological ability to actualize such control.

II. Freedom of speech: old values in the new (digital) world

1. What does freedom of speech encompass?

Before determining its scope on the Internet, we must define what is meant exactly by "freedom of speech."[8] Generally, the principle is understood as the freedom of every human expression intended for public communication. This signifies that speech, even speech that causes some measure of harm to the public, is entitled to a special degree of immunity from

government restraint. Freedom of speech is a media-independent principle. It originated in a printing press environment[9] and was elaborated on later for the purposes of radio and television.[10]

Free speech clauses developed more or less simultaneously in the United States and Europe. The First Amendment to the American Constitution was adopted in 1791. The Free Speech Clause of the First Amendment to the U. S. Constitution provides that "Congress shall make no law "abridging the freedom of speech."[11] Although directed by its terms to Congress, the clause applies equally to all levels of government.[12]

The European model for the protection of fundamental human rights is based on the existence of two distinct legal orders, namely: the legal order of the European Union ("EU")[13] and the legal order established by the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") within the Council of Europe.[14] The most important provision for European free speech protection is Article 10, ECHR. Its aim is to protect the right of everyone, regardless of frontiers, to express himself, to seek and receive information and ideas, whatever their source, as well as to impart them under the conditions set out in the text of the article 10:[15]

"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."

Similar provisions are found in the constitutions of most democratic states.

2. Restrictions on freedom of speech

Freedom of speech or freedom of expression is a fundamental right of citizens of the democratic societies. On the other hand, it also generally recognized that this right is not absolute. Free speech has never been completely unrestricted. In the course of time speech has been subjected to various restraints.[16]

In the United States exceptions to free speech rights are not encoded in the First Amendment. Instead, they are to be found in the doctrine of the Supreme Court defining the extent of free speech protection. Some forms of speech are thoroughly outlawed in the US such as fraudulent advertising, child pornography, obscenity,[17] fighting words,[18] libel,[19] speech that infringes a copyright.[20] Naturally, most of these forms of speech have a compelling government interest. Government may regulate, or censor speech if it has a compelling interest, is a public concern, or threatens national safety.[21]

The European framework for government restrictions to free speech is enacted in Article 10, para. 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. [22]

> "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."

Article 10 of the ECHR, which contains the general conditions for all free speech restrictions, irrespective of the medium they are applied to. According to the text, governmental restrictions to free speech are legitimate only if three cumulative conditions are fulfilled: state interferences restricting free speech must be prescribed by law, they must serve a legitimate purpose and they must be necessary in a democratic society. Every restriction to free speech should be proportionate to its legitimate aim. [23]

3. How the digital environment has affected how we view and exercise our freedom of speech

The key values that underlie the First Amendment remain the same both in the real and the digital world. As Professor Jack M. Balkin has noted 'the protection of individual freedom to express ideas, form opinions, create art, and engage in research, the ability of individuals and groups to share their views with others, and build on the ideas of others, and the promotion and dissemination of knowledge and opinion remain as important in a world of blogs, search engines, and social software as they did in an Enlightenment era. What has changed, however, is the technological context in which we try to realize these values."[24]

The technological revolution has drastically lowers the costs of copying and distributing information.[25] Large numbers of people can broadcast and publish their views cheaply and widely. Websites, for example, are easy to construct and easy to access. Both receiving and sending information has become easier and less costly.[26] The variety of uses and the potency of the Internet as a form of mass communication are almost unlimited.[27] E-mail's overall volume has already far surpassed that of traditional "snail" mail[28] and constitutes a prime example of the Internet's capacity for fast cheap and efficient means for the expression and exchange of ideas. Other recent developments, such as Web 2.0[29] sites range from social networking sites to virtual worlds, user-generated content platforms, peer produced-public domain encyclopedias, next-generation peer-to-peer file-sharing technologies, enhanced weblogs, and audio and video blogs (also known as podcasts and vlogs, respectively). [30] Features including blogging and YouTube, make it even easier for individuals to express themselves, either in written or video format and reach a larger audience while multimedia friendly interfaces such as MySpace allow users to be heard on a level that never would have been imaginable previously.[31] Social networking sites such as Facebook likewise provide a quick and easy way to stay in touch with friends across the globe. Internet search engines are widely used as the fastest and most effective means of obtaining a wealth of information.[32]

Ultimately, the digital revolution lowered the costs of innovating with existing information, commenting on it, and building upon it by developing common standards for storing and encoding information digitally.[33] Common standards are absolutely crucial to lowering the costs of transmission and distribution because not only do they make it easy to copy and distribute content, they also make it easier to appropriate, manipulate, and edit content[34] promoting thus innovation and creativity.

For the first time in human history content can cross cultural and geographical borders with such ease. Internet speakers can reach more people in more countries; they can interact with and form new communities of interest with people around the globe. The Internet offered people around the world access to an infrastructure for sending information worldwide, a privilege previously enjoyed only by large commercial enterprises.[35]

It has thus been argued that by lowering the costs of transmission, distribution, appropriation, and alteration of information speech has been put in the hand of an large and always increasing number of people from different countries, cultures , diverse backgrounds and strata of society.[36] This participatory nature of the new technologies has contributed to the pluralism of speech thus democraticizing speech worldwide:[37] technologies of distribution and transmission are put in the hands of an increasing number of people and increasingly diverse segments of society throughout the planet;[38] more and more people can publish content using digital technologies and send it worldwide; conversely, more and more people can receive digital content, and receive it from more and more people; equally important, technologies of innovation are available to a wider range of people. In the digital age, distribution and innovation go hand in hand.

Ironically the same aspects of technology that promote speech and innovation also promote and facilitate illegal and harmful acts.[39] The ability to copy and modify information has also led to digital piracy of protected works.[40] The conflict between between intellectual property and freedom of speech always existed, but new digital technologies have made it more salient and important. The web 2.0 raises intellectual property (IP) issues that are similar in kind to, but somewhat more complex than, those raised by more traditional Web and file-sharing technologies. Like the Web 1.0 sites of MP3.com, or Napster that preceded them, sites like MySpace and YouTube stand accused of facilitating the infringement of copyrights in thousands or even millions of songs, television shows, and motion pictures.[41] Copyright holders seek increasingly aggressive ways to protect their existing rights by promulgatin legal and technological strategies seriously affecting freedom of expression.[42]

Internet may facilitate the global communication between peoples of different cultures but it also accentuates the differences in how different peoples value speech. As professor Lessig noted in 1999 every jurisdiction controls speech it deems undesirable but what that speech is, differs from jurisdiction to jurisdiction.[43] This proves problematic in cyberspace[44] as the *La Ligue Contre le Racisme et l'Antisemitisme (LICRA) v. Yahoo! Inc.* [45] case demonstrated in 2000. In this case LICRA and other French organizations against anti-Semitism brought suit in French court against Yahoo!.[46] Plaintiffs alleged that Yahoo!'s auction site was hosting auctions of Nazi-related materials and memorabilia, the display of which within France violated French law. The French lawsuit, which involved issues of international jurisdiction and choice of law, resulted in

a French court order compelling Yahoo! to cease making available the specified anti-Semitic content to French citizens (which at that time essentially required Yahoo! to cease making this content available on the Internet at all). [47]

Yahoo! fought back in the United States by filing a suit in U.S. district court against the French organizations. The company claimed that enforcement of the French court judgment in the United States would violate the First Amendment.[48]The U.S. district court agreed, holding that principles of international comity that would generally favor enforcing international courts' judgment against United States entities were outweighed by the First Amendment values at play in this case. [49]Because the First Amendment protected Yahoo!'s dissemination of anti-Semitic speech, the enforcement of the French court order enjoining such dissemination would violate the First Amendment. [50]

III. Myths, Trends and Realities

1. Myths:

In the early days, the Internet's enthusiasts were convinced that Internet would be basically immune from state regulation. The idea was that even if states wanted to regulate the Net, they would be unable to do so, "forestalled by the technology of the medium, the geographical distribution of its users, and the nature of its content."[51] This belief that Internet is a regulation – free medium can be summarized in the three following assertions:

i. Internet cannot be regulated

The famous statement "the Internet treats censorship as a malfunction and routes around it"[52] attributed to John Gilmore,[53] one of the founders of the Electronic Frontier Foundation (EFF),[54] manifests the euphoria generated by the possibilities opened by the Internet. This was true in the nineties and it still holds some truth today mainly because of the technological structure of the Internet.[55] The Internet is basically a distributed de-centralized network , extremely hard to shut down. It appears that if a blockage is put in one place, messages will flow like water around it.[56] This idea reflected the faith in the new technology, which was bound to end censorship and move communications systems away from the control of literacy among the elite and towards multiple forms of communications.[57]

ii. Information wants to be free

Much like Gilmore's assertion above, Stewart Brand's phrase "information wants to be free"[58] further visualizes the idea that he Internet is incapable of being regulated not only because of the technology, but also because of the nature of the messages, the content, communicated through it. Internet was viewed as the ultimate communications medium which would allow ideas to "freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, […] like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation."[59] On the one hand Internet is a

realm of information, and information is very hard to regulate; on the other hand states are too slow to deal with the technology and thus control information.[60]

iii. No single state can regulate speech on the internet

The third basic belief is reflected in John Barlow's phrase, "On the Net, the First Amendment is a local ordinance." The idea was that proponents of freedom of speech , should not put their faith in the law to protect free speech; instead they should put their faith in technology.[61] It is the nature of the network technology, the nature of the informational content, and the fact that it stretches across borders beyond the control of any one sovereign all mean that speech cannot be regulated. In sum it is exactly the global nature of the Internet that is global, that is rendering it impossible for individual states to regulate speech.[62]

2. Realties: controlling the who, the what and where?

1. Generally

As we all know by now Internet can and is in fact regulated by individual states.[63] Professor Pamela Samuelson had warned as early as 1996 that the law was already threatening an important regulation of life in cyberspace.[64] Indeed, in the past years there has been a gradual change of the techno-political culture of the Internet from a cheap, effective, and global distribution network to a state driven regulated entity. [65] This is partly due to the shared concerns of many countries to exert control over the information flow for various compelling state reasons; [66] the motivations for censorship range from well-intentioned desires to protect children from unsuitable content[67] to authoritarian attempts to control a nation's access to information.[68]

2. Methods of content regulation

Professor Lessig has described the Internet in terms of the end-to-end (e2e) principle.[69] The e2e principle views the Internet much like a common carrier, simply serving as a neutral conduit for information flowing from the content provider, or "speaker," on one end to the end user receiving the information, or "listener," on the other end, [70] while it also requires that all data packets, or bundles of information, should be treated equally as they pass through the middle of the network, regardless of their content.[71] This principle, albeit consistent with the notion of the Internet as a forum promoting First Amendment freedoms[72] is not applicable in practice. The various methods of Internet content regulation developed are not always consistent with the e2e principle. [73] There are two major of the methods of content control on the Internet content, distinguishable based upon the location on the Internet where the regulation occurs.

i. End users

This method consists of regulating who are sending data packets and who are receiving them. This approach involves state-mandated controls at the end-points of the network. On the one hand, states have sought to block illegal or harmful content at its source[74] by making it illegal to send such harmful information.[75] In this sense this approach acts proactively by prohibiting

Internet users from disseminating certain information or message over the Internet. In the US such examples include the Communications Decency Act of 1996,[76] which sought to stop the transmission of pornography to minors, and the CAN-SPAM Act of 2003,[77] which disallows the sending of unsolicited commercial e-mails if certain rules are not followed.

On the other hand there is state regulation which attempts to control the receiving end of the communication by prohibiting the receipt or possession of specific content such as child pornography or copyrighted works.[78] The on going battle of the music and movie industry against internet users and P2P file sharing constitutes the prime example of attempts to control file sharing on the end user level. The industry's legal battle against individual file sharers spanned roughly five years, targeting more than 35,000 alleged file sharers in the U.S.[79] As of this writing, only two cases against individual file sharers have actually gone to trial. In *Capitol Records v. Thomas*, [80] resulted in an arguably Pyrrhic victory for the music industry plaintiffs. The Recording Industry Association of America ("RIAA") won the case on the merits in two separate trials.[81] In the retrial, the jury found against Thomas again, this time awarding $ 1.92 million, or $ 80,000 per song, in damages. Although the district court "remitted the damages award to $2,250 per song" in January of 2010, Thomas-Rassett nonetheless still faced a "reduced award" in the amount of $54,000, that is, in the court's own words, "significant and harsh."[82] In *Sony Corp. v. Tenenbaum* [83] the jury awarded the RIAA $ 675,000, or $ 22,500 per song.[84] On December 7, 2009, Judge Gertner finalized the verdict against the defendant and issued an injunction preventing him from file-sharing, but still permitted him to speak publicly about his trial. [85] The Rasset-Thomas case was the first major victory against individual file-sharers for the RIAA, which has been trying to stop file-sharing for the past ten years.[86] However, this campaign has undoubtedly proved costly and critics largely viewed the litigation as ineffective[87] damaging the reputation of the industry, widely seen as one that sues its own customers and out of step with current technology.[88] As a result in December 2008, the RIAA announced that it would no longer pursue litigation as a means of combating illegal file-sharing, although it would continue to litigate any outstanding cases.[89]

A middle of the road approach includes regulations mandating that certain content be accompanied by specific information in order to be legally sent or received. Examples of this type of regulation include again the CAN-SPAM Act which requires that certain header information is included in some messages.[90] Also, the Children's Online Privacy Protection Act of 1998 (COPPA)[91] requires that web sites implement age verification methods which prohibit Internet users from accessing certain information online unless they provide verify that users are over thirteen years of age before providing most online services. None of these first three approaches necessarily represent a substantial departure from the end-to-end principle, so long as no intermediaries, such as Internet service providers (ISPs), are required to take any action on behalf of the state to enforce the rules.

ii. Internet Service Providers

Following the admittedly unsuccessful attempt to control the end users, there has been a shift in the targets that are subject to regulation.[92] Rather than holding the actual speakers or writers to be legally liable for uttering or expressing undesirable speech,[93] the intermediary carriers in the

Internet age who have no actual knowledge of the content may also be liable.[94] Their crucial role in content regulation is inevitably associated with the architectural design of the Internet. Indeed there is only a limited number of Internet companies which possess the power to offer online services. In contrast, all users must go through an ISP before going online. Due to the setup of the Internet, the Internet Service Providers ("ISPs") are situated in this powerful and influential position making them the perfect target for state-mandated regulation and/or self-imposed content censorship.[95] Because of pivotal role ISPs play in content regulation we shall examine their role in more detail.

ii.a. Safe harbors:

It has to be noted that because of the Internet's unprecedented speech-facilitating characteristics and the pivotal role that Internet Service Providers play in channeling such speech the issue of shielding ISPs from liability based on the third-party generated content -especially in the area of copyright law- arose early. Although internationally, a multinational treaty directly addressing the issue of ISP safe harbors does not exist, numerous domestic regimes which reject strict liability for safe harbors so long as ISP's are not directly involved in the creation of the illegal or censored content are implemented. For instance Section 230(c)(1) of the Telecommunications Act of 1996 provides that "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."[96] Accordingly, Internet intermediaries like network providers and online service providers but also websites or online services on which other people provide content (chat rooms, blogging services, website hosting services, search engines, bulletin boards, or social networking sites like Facebook and Myspace, cannot be held liable for what other people say when others use these networks, services, or sites.[97] This privilege applies to a wide range of different communications torts and crimes but not to alleged infringements of intellectual property rights. In these cases, the safe harbor provisions of the Digital Millennium Copyright Act apply.[98] Under the DMCA, no copyright action may lie for damages against companies providing Internet connectivity or transmitting or routing material over the Internet provided the ISP is not involved in the creation of the content in question.[99]

Similarily, in the European Union the Electronic Commerce Directive (ECD) erects safe harbors for online intermediaries.[100] Under the ECD providing access to a computer network or transmitting information over it, including engaging in the transient storage or reproduction of the information for transmission, shall not give rise to monetary liability irrespective of notice of illegal activity[101] as long as "[the provider] does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or ... upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information." [102]

ii.b. Government mandated regulation

One of the most effective methodologies to control internet content to date appears to be placing pressure on the internet service provider. Unlike the attempts to regulate thousand or even millions of end users, ISPs are likely to provide effective, efficient, and economic means of

control. As a result, ISPs are enlisted to block or to inspect packets of information.[103] On the other hand, the corporations find themselves required to comply with rules in jurisdictions in which they are doing business and whose views on freedom of expression may be entirely different from their home countries. [104]

ii.b.1. ISPs as state-mandated censors:

The most common method to regulate undesirable content on the Internet is through Internt filtering.[105] This is the original and best understood form of Internet censorship. Internet users on a particular network are blocked from accessing specific websites.[106] Internet filtering generally describes technical approaches to control access to information on the Internet. There are three commonly used techniques to block access to Internet sites: IP blocking, DNS tampering, and URL blocking using a proxy.[107] These techniques are used to block access to specific WebPages, domains, or IP addresses.[108]

However, there are two inherent flaws associated with all internet filtering technologies: underblocking, in which case the filter is simply ineffective, and overblocking, when the technology implemented blocks content it did not intend to block.[109] The problem lies within the limitations of the current technology [110] since current technology is not able to accurately identify and target specific categories of content found on the billions of web pages and other Internet media [111] often resulting in blocking unrelated websites. In reality, when ISPs are required by state regulations to filter objectionable materials, they have to respond quickly and tend to adopt the cheapest means to do so, resorting to filtering by IP address.[112] However the unintended consequence is that if the target Web site is hosted in a shared hosting server, all websites on the same server will be blocked [113] resulting in filtering out numerous unrelated web sites.[114] For instance, South Korean ISPs were required to block thirty-one web sites by the authorities, but in choosing to block by IP address, 3,167 unrelated domain names hosted on the same servers were blocked as well.[115] This problem of over-blocking by ISPs' has been described by Zittrain as a crude form of Internet discipline, amounting to a form of "Internet death penalty." [116]

China is notorious for having implemented the most sophisticated system of Internet censorship and surveillance in the world. [117] The ‘great firewall of China’ uses a variety of overlapping techniques for blocking content containing a wide range of material considered politically sensitive by the Chinese government. While China employs filtering techniques used by many other countries, including DNS (domain name system) tampering and IP (internet protocol) blocking, it is unique in the world for its system of Internet connections when triggered by a list of banned keywords. Known as a TCP reset, this content filtering by keyword targets content regardless of where it is hosted.[118] Any foreign internet company wishing to penetrate the immense Chinese market have to adhere to the strict content regulation requirements mandated by the Chinese government [119] and internet giants such as Google, Microsoft and Yahoo! are no exception.

As a result, Internet users in China have access to a “sanitized” version of search results.[120] The type of content that is targeted for blocking is wide-ranging and covers social, cultural, security

and political topics considered a threat to Communist Party control, and social and political stability. [121] Websites that are almost always filtered include the ones containing content related to Taiwanese and Tibetan independence, Falun Gong, the Dalai Lama, the Tiananmen Square incident, opposition political parties or a variety of anti-Communist movements[122] but also the web sites of major news organizations, such as the BBC, as well as international advocacy organizations, such as Human Rights Watch.[123] Up until recently a search request for the Tiananmen Student Movement at Google.com would yield pictures of rolling tanks, whereas only smiling faces of passers-by would appear at Google.com.cn.[124] As a Citizen Lab [125] study of four popular search engines in China found, the total number of censored sites may not be that high, especially when compared to the amount of indexed sites, however the impact of their exclusion cannot be underestimated since the censored sites are often the only sources of alternative information available for politically sensitive topics.[126] Without knowing what has been filtered and the alternatives available, users are forced into a "digital deceit,"[127] without even realizing that they are living in different Internet universe.

Until recently Google defended its practices in China arguing it would do more harm than good to not participate in countries notorious for their hostility to free speech.[128] However, this changed in early 2010 when Google announced its decision to stop operating in China.[129] Specifically, in January 2010 Google decided to stop censoring search results in China, after discovering that someone based in that country had attempted to hack into the e-mail accounts of human rights activists. [130] Although no direct accusation against the Chinese government was ever made, Google stated that the attacks, combined with attempts by China over the last year to "further limit free speech on the web," led it to conclude that it needed to "review the feasibility of [its] business operations in China."[131] In March 2010 Google shut down its Google.cn site and has been redirecting users to Google.com.hk, where it offers uncensored Chinese-language search services.[132] While Google ended its own self-censorship in China, searches within the .hk Google, albeit not censored by Google, will still be affected by China's keyword filtering, i.e. searches for certain terms will not get through to google.com.hk search engine and the end user in China will not get any results.[133] The difference is that the user now experiences the censorship first hand.[134] Despite Google's rhetoric about protection of freedom of expression in China it is questionable whether the company would have decided to stop its operation in China had it not been the victim of the December 2009 cyber-attacks.

Apart from filtering there are several instances where governments get involved directly requesting removal of specific content. Indeed since the infant stages of the internet government have called upon ISPs to removing undesirable content. For instance, in 1995, the German Government requested CompuServe to remove porn sites from its servers a request to which Compuserve ultimately complied by implementing a content filtering scheme on a country-by-country basis.[135] Similarly in 2001, Google removed pro-Nazi and racist sites from search results in its localized search engine, following requests of the French and German governments.[136]

In 2008, following a civil court judgment in Civril, Turkey access to a photo and media-sharing service, Slide, closed to all Turkish citizens because some material deemed insulting to the country's founder, Ataturk, was posted.[137] The same year, the Indonesian government ordered the country's internet service providers to bock YouTube for publishing the 15-minute anti-

Muslim film “Fitna”, made by Dutch MP Geert Wilders, leader of the anti-immigration Freedom Party (PVV). Some of the country's ISPs followed the block order, but “Fitna” could still be viewed through other providers.[138] That same year following riots in Tibet, China shut down access to YouTube inside the country in an effort to contain the news.[139] In late February 2008, Pakistan’s telecoms regulator ordered a ban of You Tube after a “blasphemous” speech critical of Islam was posted. Pakistan’s blocking of YouTube was so effective that disabled access to the popular site everywhere in the world for a few hours.[140] More recently, in May 2010 Pakistan imposed a ban on the social networking site Facebook amid anger over a page that encouraged users to post images of Islam's Prophet Muhammad.[141] This ban was lifted only after officials from the social networking site apologized for the offensive to Muslims page and removed its contents.[142]

ii.b.2. ISPs as State-Informers

A more troubling trend is that increasingly state governments rely on ISPs to retrieve information about internet users, thus employing ISPS as informers or the "secret police" of the Internet.[143] A few of the most notorious cases of corporate involvement in assisting the a government arresting and condemning four dissidents — Shi Tao, Li Zhi, Jiang Lijun and Wang Xiaoning — to prison for terms of up to 10 years involves Internet giant Yahoo!

In 2004 Yahoo, turned over information about the Chinese journalist, Shi Tao, to the Chinese authorities.[144] In April 2004 Shi Tao used an anonymous identity to send by his Yahoo! email account[145] the content of "A Notice Regarding Current Stabilizing Work" to the "Asia Democracy Foundation" in New York.[146] The content of the document essentially warned journalists that overseas pro-democracy Chinese dissidents may come back to mainland China during the 15th anniversary of the Tiananmen Square Protests of 1989 on June 4, which would affect the politico-social order's stability and asked all news media to not report anything regarding the so-called "June 4th event", Falun Gong or people calling for politico-social change. The Chinese government obtained the account holder's information, which described the IP address, the corresponding user information, Shi Tao's telephone number, and the location of his terminal, by Yahoo! (Holdings) Hong Kong Ltd. ("Yahoo! (HK)")[147].In April 2004, charged with the offence of illegally providing state secrets outside the country in violation of Article 110 of the Criminal Code of the People's Republic of China ("PRC").[148] On April 30, 2005, Shi was sentenced to ten years imprisonment.[149]

Yahoo! defended itself, stating that it had not betrayed its users, but that it had to operate within the law, regulations, and customs of the country in which it is based or else it would have no alternative but to leave the country.[150] Some months later, it was discovered that the document provided to Yahoo! China on April 22, 2004 by the Beijing State Security Bureau actually stated, *“Your office is in possession of the following items relating to a case of suspected illegal provision of state secrets to foreign entities…”*[151] directly contradicting the sworn Congressional testimony by Yahoo! Senior Counsel Michael Callahan in February 2006.[152]

After Shi Tao's story attracted publicity world-wide three other cases in which Yahoo! provided information to Chinese authorities about people who used Yahoo! China e-mail accounts to

transmit political information were revealed: Wang Xiaoning, a Chinese engineer by profession, who posted electronic journals in a Yahoo! Group calling for democratic reform and an end to single-party rule; [153] Li Zhi, a former government worker who criticized the Communist Party in online discussion groups and encouraged others to join the China Democracy Party.;[154]and Jiang Lijun, a Chinese freelance writer who posted articles on the Internet advocating a multiparty system of government . All were tried and sentenced in 2003 – one year before Shi's arrest. In all three cases, Chinese court documents cite Yahoo! Holdings (Hong Kong) as the source of information about the defendants' Chinese Yahoo accounts.[155]

On August 28, 2007, the World Organization for Human Rights USA sued Yahoo! under the Alien Tort Statute for Xiaoning' alleging that Yahoo! "knowingly and willfully aid[ing] and abett[ing] in the commission of [plaintiffs'] torture" by providing the Chinese authorities with information, including plaintiffs'e-mail records IP addresses and user identification numbers, that caused the arrests of writers and dissidents.. [156] On November 13, 2007, Yahoo!, Xiaoning, , along with Shi Tao, who was later named as an additional plaintiff, settled the lawsuit for an undisclosed amount[157] leaving questions raised about corporate liability unanswered.

Similarily, in 2007, Google was alleged to have handed information of its user, who had posted insulting images of god Shiva on its social networking site, to the Indian government. Ironically, Google passed the wrong information to the authority, leading to the arrest of an innocent person. [158] Again in 2008, a 22-year-old tech worker in a suburb of Delhi, posted on a comment titled "I hate Sonia Gandhi" in an Orkut community through an Orkut account associated with his Gmail account. Law enforcement immediately took action and Google not only did it take down the material but also gave the user's IP address to police, allowing them to track down his physical location leading to the user's arrest.[159] Google wouldn't disclose what precisely was posted about Ms. Gandhi, but said it determined the material violated India's obscenity laws.[160] The company said it supported the free expression of its users and is committed to protecting user privacy, but the company complies with local laws and valid legal process, such as court orders and subpoenas.[161]

In 2006, in United States, a country famous for its liberal views on freedom of speech, it was revealed that AT&T was cooperating with the National Security Agency surveillance program of the U.S. Government to monitor communications of its citizens with suspected terrorist ties outside of the United States. [162] The Electronic Frontier Foundation ("EFF") sued the telecommunications company on behalf of its customers for violating privacy law by collaborating with the NSA in the massive program to wiretap and data-mine AT&T's users' communications. In June 2009, a federal court dismissed this and dozens of other lawsuits against telecoms, ruling that the companies had immunity from liability under the controversial FISA Amendments Act (FISAAA), which was enacted after the filing of the case.[163]

Google has had its own battles with the government. In August 2005, the U.S. government ordered the company to comply with a subpoena that would provide "a multi-stage random sample of one million URL's" from Google's database, and a computer file with "the text of each search string entered onto Google's search engine over a one-week period (absent any information identifying the person who entered such query" to implement the Child Online

Protection Act.[164] In the end, the Justice Department came to a compromise by requesting merely fifty thousand URLs and five thousand search queries, and finally only looking at ten thousand and one thousand, respectively[165] which also raises a question about the arbitrariness of the initial request.

Although it is well known that communications or customer records that are in storage by third parties, such as email messages, photos or other files maintained in the cloud by services like Google, Microsoft, Yahoo Facebook and MySpace are routinely disclosed to law enforcement, and there is no legal requirement that statistics on these kinds of requests be compiled or published.[166] As a result, there is currently no way for academic researchers, those in Congress, or the general public to determine how often most email, online photo sharing or social network services deliver their customers' data to law enforcement agents.[167] Security and privacy analyst Christopher Soghoian filed Freedom of Information Act requests with several parts of the Department of Justice in the summer of 2009, in an attempt to follow the "money trail" in order to determine how often Internet firms were disclosing their customers' private information to the government.[168] Comcast and Cox did not object but both Verizon and Yahoo! resisted disclosure of such information. Verizon first revealed in its objection letter that it "receives tens of thousands of requests for customer records, or other customer information from law enforcement" and claimed among others that its customers might "become unnecessarily afraid that their lines have been tapped, or call Verizon to ask if their lines are tapped."[169] Yahoo! claimed that if such information is disclosed "would be used to "shame" Yahoo! and other companies -- and to "shock" their customers" and impair the company's reputation. [170]

Finally in April 2010 Google announced the launch of the new Government Requests tool [171]"to give people information about the requests for user data or content removal received from government agencies around the world" stating the belief that this tool will promote " greater transparency", will enable discussions about the appropriate scope and authority of government requests and that other companies will make similar disclosures.[172] Although there are limits to what this data actually discloses to the public[173] it is an imperfect yet significant step toward transparency.

ii.c. Private censorship or self-regulation

Besides government mandated regulation Internet providers customarily proceed to content restrictions amounting to self-regulation, in other words a form of private censorship. The vast majority of Internet access and service providers, which are privately owned, assert and exercise substantial control over the expression that flows through their conduits.

First there is a matter of transparency with regards to the specific criteria used in the different filtering regimes.[174] Since one of the flaws of filtering regimes is overblocking, collateral filtering albeit unintended, necessarily means that both the ruling authorities and the public may not even know what has actually been filtered, rendering commercial companies who have the technical know-how to the ultimate decision makers.[175] Moreover, since most companies consider and treat commercial filtering technology and block lists as the intellectual property of the manufacturers and ISPs, to which the public cannot have access[176], the chance of challenge is minimal. As a result there is practically no accountability for the ISPs filtering practices which

maybe vague and arbitrary.[177]In essence ISPs are in a position which allows them to broadly restrict access to the Internet which in turn means that the ISPs are in fact determining who can be online, what can be viewed, and who can say what is on a what was originally considered a free-for-all medium.[178] Taking this into account it arguable that ISPs are no longer mere conduits or neutral intermediary carriers.[179]

Transparency is equally absent in the way search engines work. Search engines occupy a position of central importance on the Internet.[180] The percentage of internet users who use search engines on a typical day has been on rise since 2002 estimating that the number of those using a search engine on a typical day is closer to the 60%[181] and the major search engines, Google and Yahoo!, and Bing ranked as the three most used websites in the United States.[182] The rise in the importance of search engines in online communications is reflected in the increased litigation involving demotions in the website ranking or search engine's refusals to include advertisements.[183] The importance of search engines is also reflected in the energy that webmasters put into ensuring that they are included in search engine indices and in attempting to improve their ranking within search results.[184] Certain forms of bias seem inherent in the structure of the search engines. For instance when search engines build their indices using automated software agents ("bots") which follow hyperlinks between websites, [185]and search engines use the number of links to a site as a proxy for its quality,[186] the link structure of the Web may favor popular and highly- linked sites.[187]However, most of the debate focuses different forms of bias introduced by search engines, including the removal of websites from the search engine index, the reduction of website ranking, the refusal to accept keyword-triggered advertisements from certain websites, and the practice of providing preferences in indexing or ranking for paying websites.[188] Several authors have noted the problem of bias in search engines, although they differ widely in their recommended solutions.[189]Several have called for a transparency requirement to be imposed on search engines. This transparency requirement should include (a) disclosure of the way in which the search engines work and how they rank search results, [190](b) clear identification of paid links, [191]and (c) notification when information is blocked or removed pursuant to law.[192]

Secondly, each of the major ISPs establishes and enforces Terms of Service by which it sometimes prohibits the expression of certain types of speech that are considered protected speech. AOL, for example, specifies in its terms of Service that AOL and its agents "have the right at their sole discretion to remove any content that, in America Online's judgment ... [is] harmful, objectionable, or inaccurate."[193] AOL enjoys the discretion to censor constitutionally-protected speech in its discussion forums and other online spaces, including "vulgar language or sexually explicit conduct ‘’ that it describes as being as appropriate as they “ would be at Thanksgiving dinner” and warns that " AOL makes the final determination about whether content is objectionable or not. [194]

Similar restrictions on speech are imposed by most if not all major ISPs making practically impossible for Internet users seeking stronger protection for their expression to “shop around” and chose a different ISP. For Instance Yahoo!'s Terms of Service, [195] prohibit users from

making available content that is"objectionable," and warns that Yahoo! may pre-screen and remove any such "objectionable" content.[196] Comcast prohibits users from disseminating material that "a reasonable person could deem to be objectionable, embarrassing, ... or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful."[197] also stating in its Terms of Service,that it "reserves the right ... to refuse to transmit or post and to remove or block any information or materials ... that it, in its sole discretion, deems to be ... inappropriate, regardless of whether this material or its dissemination is unlawful." [198]

Internet Providers policies may also further restrict free speech. In 2008 Google was accused that its "excessively restrictive policies" have resulted in the censorship of lawful advertisements that educated and informed the public.[199] An activist who wished to place an advertisement stating "AT&T has given $7,500 since 2004. Who else has donated to the senator?" to be displayed when Internet users searched for the name of a particular politician was censored by Google. Google informed the user that the ad campaign run for the previous months was being terminated due to a trademark complaint by AT&T.[200]

In the United Kingdom, Google was reported to have 'delisted' Inquisition 21st Century, a website campaigning against many of the Operation Ore child pornography convictions in the U.K.Kingdom suggesting Inquisition 21 had attempted to manipulate search results.[201] In 2008, Google refused to run ads for a UK Christian group opposed to abortion, explaining that "At this time, Google policy does not permit the advertisement of websites that contain 'abortion and religion-related content."[202]

Profesor Dawn Nunziato cites several more examples, including Google's suspension of ads for W. Frederick Zimmerman, once it became aware of the content of the author's book - Basic Documents About the Detainees at Guantanamo and Abu Ghraib- advertised via his sponsored link. [203] Google cited its policy not permiting "the advertisement of websites that contain "sensitive issues"; Google's suspension of ads for a website that contained an article criticizing President Bush on the ground that ads advocating against an individual violate its polic; Google's refusal to run the ad of Unknown News for anti-Iraq-war bumper stickers on Google's Sponsored Links with an ad headlined "Who Would Jesus Bomb?" . Google finally agreed to reinstate it if the website was edited ""to show both sides of the argument' over attacking Iraq."[204]

Third, network providers might discriminate the content and applications of favoring some speakers and businesses over others by blocking access to certain[205] sites and services or permit access to end-users only if these sites or services pay a special fee.[206] Major Internet companies including Google , AOL, and EarthLink exercise great editorial control and impose what in essence is speech regulations especially with regards to sponsored links.[207] Google is known for having refused to host a range of politically-charged, religious, and critical social commentary in the form of advertisements themselves, as well as the websites to which these advertisements link. Google has also required prospective advertisers to alter the content within their sponsored links - as well as within their websites - as a condition for Google's hosting such content. One of the most notorious cases involve Google when in 2002 it removed websites that critical of the Church of Scientology. This incident sparked numerous complaints from Internet users and

groups to Google, and the links to the banned site were restored.[208] Google subsequently began to contribute its notices to chillingeffects.org, archiving the Scientology complaints and linking to the archive. However more cases soon followed. For instance in 2003, Google stopped showing the advertisements of Oceana, a non-profit organization protesting a major cruise ship operation's environmental policies under the headline "Help us protect the world's oceans," citing its editorial policy at the time, stating "Google does not accept advertising if the ad or site advocates against other individuals, groups, or organizations."[209]

Additionally, Internet providers might seek to control certain heavily trafficked sites - like eBay, Google, or sites that use considerable bandwidth[210] to ensure that their traffic flows smoothly to end-users.[211] In 2007, after independent testing by the Associated Press, later confirmed by EFF, it was discovered that Comcast began engaging in protocol-specific interference with the activities of its subscribers, specifically with BitTorrent, Gnutella, and potentially other common file sharing protocols employed by millions of Internet users.[212] Comcast claimed that it performed "network management" that might interfere with particular subscribers in rare circumstances, but it did not block or target any application or protocol. [213] The Federal Communications Commission (FCC), intervened and asserted jurisdiction over Comcast's network management policies and ordered Comcast to cease discriminating against peer-to-peer network traffic. On April 6, 2010, the DC Court of appeals in a unanimous 3 panel decision vacated the Federal Communication Commissions's 2008 order against Comcast.[214] The Court did not reach the question of whether Comcast had wrongfully interfered with its subscribers' use of internet services like file sharing and Skype; instead it held that the F.C.C. lacks statutory authority to regulate broadband services. According to news reports, the court's decision will make it more difficult to enact legislation safeguarding net neutrality.[215] Following this decision, the FCC announced that it was "seriously considering" placing the internet industry in the same c ategory as the telecommunications industry, a highly regulated industry that will further limit ISP neutrality.[216] Many are concerned with the potential ramifications of such a reclassification. On May 2010 a group of 171 House Republicans May 28 sent a letter to Federal Communications Commission Chairman Julius Genachowski protesting a plan to reclassify broadband internet access as a "telecommunications" service.[217]

This decision sparked once more the debate about net neutrality. The principle of network neutrality holds that, in general, network providers may not discriminate against content, sites, or applications. [218] The goal of network neutrality is to keep digital networks open for many different kinds of content and for many different types of applications and services that people may devise in the future.[219] But when talking about the role of Internet or network providers in the debate over network neutrality, we have to realize that discrimination against certain types of content or services is not so much based on their politics or their moral tone (although there have been exceptions).[220] Most ISP-imposed discrimination will be for economic reasons - to favor business partners and protect their business models.[221] Internet providers might want to give a traffic advantage to their content partners or to their own content, [222] reserving a fast track for favored content partners; conversely, network providers would not protect the flow of content (or even slow down content) from non-partners, competitors, amateurs, and end-users. [223]

Probably the most ironic instance of self-censorship, arguably based on business considerations, is Yahoo!'s case against La Ligue Contre le Racisme et l'Antisemitisme . After Yahoo! won a highly publicized international battle on behalf of free speech values in *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, [224] Yahoo! chose, apparently based on commercial considerations, to prohibit the dissemination of the Nazi-related content at issue in the case. [225] Other U.S based Internet search engines and service providers also refuse to host Nazi-related and other controversial content, even though such speech is protected by the First Amendment against government censorship.[226]

III. Current Trends: putting the pressure on ISPs

The analysis above demonstrates the ways in which private entities, including Internet providers like Google, AOL, and Yahoo!, have broadly exercised the power to regulate and censor speech on the Internet.[227] These companies serve as conduits for the speech of others since internet users depend on them for access to other speakers[228] making them the ideal point of control for restricting online speech.

Probably the most prominent attempt at censoring content on the internet stemmed from the battle of the music industry against peer to peer file trading. That conflict has always existed, but new digital technologies have made it more salient and important.[229] This battle continues to this day and the music and movie industry has been the driving force in introducing and implementing speech regulations throughout the world. Like most of the developments involving the protection and censorship of speech on the internet there is both positive and negative results. On the one hand most jurisdictions have implemented safe harbors for internet service providers[230] shielding them from liability for the actions of their end users, so long as they were not actively involved in the posting or dissemination of the allegedly illegal content beyond the mere provision of services. On the other hand the same developments have also affected adversely speech.

i. Copyright v. anonymity

The first step in restricting infringement of intellectual property rights is to identify the infringer. Thus the Music industry promoted early the adoption of legislative regimes which would facilitate identification of the alleged infringer. In United States, the copyright owners have a critical weapon in their arsenals recent against illegal sharing of copyrighted work, the abbreviated subpoena procedures established in Section 512(h).[231] Under Section 512 (h) copyright owners have the ability to obtain a subpoena on request from a clerk of a United States District Court for disclosure by a service provider of the identity of a subscriber who has allegedly engaged in copyright infringement. [232]

Unlike the notice and take down provisions of Section 512(c), [233]there is no requirement that subscribers whose identity is being sought be notified of the subpoena or given an opportunity to challenge its propriety prior to disclosure of their identity. [234]Moreover, such subpoenas are issued as a ministerial act of the clerk of the court, without the need for, or benefit of, judicial

oversight. [235]Following the court decisions in the Recording Industry Ass'n of America, Inc. v. Verizon Internet Services,[236] where the court held that §512(h) applied only to ISPs that stored infringing data on their servers, not ISPs that acted solely as intermediaries[237] RIAA's ability to use § 512(h) to obtain contact information about accused infringers was limited forcing RIAA to commence what became known as its "John Doe" lawsuits. [238]

In Europe, the European Court of Justice also struggled with the communication of personal data in the context of civil proceedings.[239] In the famous case of Promusicae v. Telefonica de Espana SAU (Telefonica), [240] Plaintiff, Promusicae, a Spanish consortium of music and video producers, requested that Spanish ISP Telefonica reveal the identity of certain subscribers suspected of illegal file-sharing. After a Spanish court granted the request, Telefonica filed an appeal arguing that European law barred it from sharing personal data with Promusicae.[241] The Spanish Court of Appeal in Madrid referred the matter to the European Court of Justice on the issue of whether Promusicae violated EU law. The court considered whether, under Council Directive 2004/48 on the enforcement of intellectual property rights, and Articles 17(2) and 47 of the Charter of Fundamental Rights of the European Union, member states must require ISPs to disclose personal data to third parties in cases involving copyright violations. The court held that there is no such requirement. [242]The ECJ ruled that Member States have no obligation to require an ISP to disclose information to a rights holder in civil proceedings.[243] The ECJ left the decision to be balanced between the competing rights of intellectual property rights and privacy rights.[244] In the end the ECJ noted that the obligation to protect right holders private information should not be leveraged or expensed against the cost of data protection[245] invoking the principle of proportionality in urging member states to strike a fair balance among the various fundamental rights protected by the Community legal order.[246]

ii. Three strikes or graduated response scheme

ii. a Legislative Provisions

The RIAA's campaing against individual users, also known as the "John Doe' campaign, proved largely unsuccessful and generated a lot of bad publicity for the music and movie industry. As a result, this industry adopted a new response: the graduated response plan, which threatens users with the possibility of losing their access to the Internet, rather than with the threat of lawsuits.[247] This approach, known as the "three strikes"[248] or graduated response plan,[249] involves both the music industry and the ISPs. The music industry monitors and notes IP addresses of alleged infringers and notifies the respective ISPs.[250] In turn, ISPs then contact the users and give them three chances to stop their infringing activities.[251] Failure to comply with the warning to stop, will result in the ISP's suspending the users' Internet access through the ISP's server.[252] In order for the RIAA's new anti-piracy initiative to succeed, the RIAA needs cooperation from regional ISPs.[253]

In the United Sates , if ISPs do not agree to implement a graduated response plan, however, the RIAA could compel them to comply by invoking 17 U.S.C. § 512(j)(1)(A)(ii). This subsection of the DMCA permits the copyright holder, to go to court and get:

> "an order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order."[254]

Although the copyright holder must get a court order to terminate Internet access, a preliminary injunction can be issued without a trial.[255] In addition, the injunction is issued against the ISP, rather than the user thus depriving the end –user his or her day in court.[256] ISPs who refuse to cooperate which might also be threatened with liability, under § 512(j).[257] Section 512(j) thus creates a system where copyright holders can get an "extra-judicial temporary restraining order, based solely on the copyright holder's allegation of copyright infringement." [258]

The music industry's new initiative has been more successful in Europe where it has resulted in the adoption of legislation incorporating and implementing the graduated response plan. In 2007 the French government requested a commission led by Denis Olivennes to negotiate an agreement between organizations representing the music and film industry and internet service providers on proposals to combat unlawful file-sharing.[259] This process resulted in a controversial legislation known as HADOPI, named after the government agency created by the resulting law (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet)[260]. The purpose of this bill was to implement a so-called *riposte graduée* or graduated response. Upon request on behalf of the copyright owner, HADOPI would request that the relevant ISP to provide the contact details of the subscriber whose IP address is under investigation and send an email recommendation to the subscriber concerned advising the user of the danger of acts of infringement and of the existence of security devices. If, during the six months following this first recommendation, similar violations are recorded, a second recommendation may be sent by letter with acknowledgement of receipt. Failure to comply would enable HADOPI order suspension of internet access for the user in question. This last provision caused the Constitutional Council's to strike down the original HADOPI law.[261] Council reasoning that only a judge may order the suspension of internet access not an independent administrative authority such as HADOPI.[262] Soon thereafter, the French government proposed HADOPI 2 to Parliament instituting a judicial process[263] prior to ordering internet suspension but essentially keeping the main provisions of the original law intact. HADOPI 2 passed constitutional muster on October 28, 2009.

Similar to HADOPI Law, the United Kingdom, recently enacted the Digital Economy Act.[264] Under this act, passed on April 8, 2010,[265] ISPs will be required to send warning letters to any individual users suspected of illegally downloading copyrighted files after receiving sufficient evidence from a copyright holder that unlawful copyright infringement is taking place.[266] Ofcom, which regulates the U.K.'s broadcasting, telecommunications and wireless communications sectors, is given the authority to take tough measures combat unlawful P2P file sharing. The Digital Economy Act empowers Ofcom to use tougher measures to combat unlawful P2P file sharing. If a system of warning letters to alleged pirates fails to reduce online infringement substantially within 12 months,[267] Ofcom can then have ISPs hand over the alleged infringers' names and addresses so the copyright holders can serve them with a court injunction,. ISPs can also be required under the new law to implement technical penalties, such as reducing Internet

download speeds, blocking web sites, and suspending internet access to individual users.[268] However, following strong critism[269] and after public pressure it has been speculated that the coalition government taking over in the UK, some may decide to repeal or modify the Digital Economy Act.[270]

Other countries are also in the process of introducing similar laws. New Zealand after an initial unsuccessful attempt to pass its own version of "three strikes" law in 2008[271] returned with an updated version of the law in 2010.[272] On March 2010, Belgian senator Philippe Monfils presented a new version of his proposition for a law that would implement in Belgium the graduated response system in illegal downloading cases, as the one introduced by the Hadopi law in France. The Belgium draft law includes blocking of websites via ISP, similar to the French system introduced by Hadopi law.[273] Similar laws and policies have been considered even if ultimately rejected by by Australia, Hong Kong, Germany, the Netherlands, South Korea, Sweden, and Taiwan. [274]

ii.b. Voluntary Collaboration

To achieve efficiently function of the graduated response plan the copyright holders must have the full cooperation of ISPs in withholding services from repeat infringers. The reaction of ISPs seem to vary between acceding to the RIAA's demands for fear of being found contributory liable, and protecting users' rights and their own business interests. [275] AT&T, a large ISP, agreed to work with the RIAA to stop file-sharing [276] forward takedown notices to users without suspending their Internet service, [277]but it is unclear whether it will go further to aid the RIAA's initiatives. Similarly, in December 2009, Verizon announced that it would begin forwarding copyright infringement notices it receives from copyright holders [278] according to which, if Verizon receives multiple notices regarding alleged infringement, these users might "risk having their Internet service interrupted or turned off and [face] serious legal consequences if the copyright owner decides to sue over the alleged infringement." [279] On January 20, 2010, Verizon admitted that it had cut off service to a number of people who had been accused of sharing files. The Verizon spokesperson, Bobbi Henson, disclosed that Verizon had "cut some people off".[280]

In June 2008, Virgin Media began sending "educational" letters to thousands of Internet subscribers alleged to be file sharing illegally,[281] n a joint effort between Virgin Media and the British recording industry association, warned the recipients that file sharing would ultimately result in termination of their accounts.[282] Shortly afterward, it was announced that five more of Britain's largest Internet intermediaries had followed Virgin Media's lead and would begin their own "educational" letter campaigns.[283]In addition to threatening subscribers that illegal file sharing could lead to suspension or termination of Internet service, subscribers were warned that their online activities could be monitored and their Internet connection speeds could be degraded to make file sharing impractical. [284]

In May 2010, Eircom, the largest ISP in Ireland, announced that it would start cutting repeat accused copyright infringers off the Internet, appearing to be the first ISP in Europe to implement a voluntary "three-strikes" regime of graduated response.[285] This decision was the result of a settlement reached between IRMA (the Irish Recorded Music Association) and

Eircom after a lawsuit filed by IRMA trying to hold EIRCOM liable for copyright violating users.[286] It is expected that, during the pilot phase, Eircom will process about 50 IP addresses a week.[287]

ii.c. Criticism:

The three strikes approach has been widely critised. First it has been argued that the new graduated response plan is particularly troubling not only because it allows cut off Internet access to users without a trial, but also because the methods used to identify the users are notoriously faulty.[288] Professor Peter Yu cites several instances of internet users having been subjected to unverified suspicion of infringing activities through unreliable technologies including the case of a sick teenager who was sued for sharing ten songs via peer-to-peer networks when she was in hospital receiving weekly treatments for pancreatitis, and an 83-year-old deceased woman who did not use computers during her lifetime.[289]

Second many commentators consider that these laws will be difficult to enforce, that there will always exist a way to circumvent the laws and that only "occasional" (as opposed to persistent) pirates will be convinced by these laws to stop unlawful downloading. In any case, at this stage, no recommendation has yet been sent by HADOPI.[290] Moreover, in response to the graduate response scheme Pirate Bay[291] reminded internet users that its VPN is ready and willing to help them when they need it at a low fee. [292]

In addition, a new study carried out by the University of Rennes on the illegal downloading of online music and video in France revealed that it grew by three per cent between September and December 2009 - despite the passing of HADOPI law specifically designed to curb this practice.[293] It also concluded that the suspension or permanent removal of an individual's Internet connection will be counterproductive as many who do pirate content also pay for items online as well.[294]

It also has to be noted that several jurisdictions, including Hong Kong, Germany, Spain, and Sweden have explicitly rejected the graduated response plans over concerns about the copyright holders' attempts to use the copyright laws to defend old business models and unknown implications. [295] In Australia in a recent court decision in a case involving the Australian Federation Against Copyright Theft (AFACT) against the Australian ISP iiNet, facilitating infringement of copyright it was determined that "*The Court does not consider that warning and termination of subscriber accounts on the basis of AFACT Notices is a reasonable step, and further, that it would constitute a relevant power to prevent the infringements occurring […][I]t would seem that termination of accounts in the circumstances of unproven and sporadic use, at least absent judicial consideration of the extent of the infringement on each account, would be unreasonable."*[296]

On November 5, 2009 European Union lawmakers and Member State governments Nov. 5 agreed on safeguards against the suspension of Internet service to users merely suspected of copyright violations. The compromise agreement, contained in a telecommunications reform package, stated that restrictions on a user's internet access may only be taken "with due respect

for the principle of presumption of innocence and the right to privacy."[297] There must be "a prior, fair and impartial procedure" guaranteeing "the right to be heard." Commissioner Reding said on this matter: "The new internet freedom provision represents a great victory for the rights and freedoms of European citizens[…] 'Three-strikes-laws', which could cut off Internet access without a prior fair and impartial procedure or without effective and timely judicial review, will certainly not become part of European law."[298] … In addition in April 2010 the European Commission welcomed the decision to make the draft of the Anti-Counterfeiting Trade Agreement (ACTA) available to the public clarifying that "no party in the ACTA negotiation is proposing that governments should introduce a compulsory "three strikes" or "gradual response" rule to fight copyright infringements and internet piracy."[299]

V. Final remarks

It has been said that "the spread of information networks is forming a new nervous system for our planet."[300] It is also true that despite repressive regimes' attempts to suppress information, in many respects, information has never been so free. Information networks are finding a way to get through and allow people discover new facts thus making governments more accountable.[301] It is equally true that it is rather unlikely to achieve an international consensus on freedom of speech on line and what that entails due to the highly diverse cultural, political, religious ethnical and social-economical backgrounds of the different countries around the world. On the other hand most of the implementation of the censorship methods have been placed on private companies which are not always accountable as to their business dealings. It has become apparent that although private sector companies have a responsibility to respect and uphold the rights of customers and users, they cannot be expected to undertake on their own the task of resolving the political issues that threaten free expression on line.[302] His task requires a multi-sectoral approach and decisive legislative initiatives.

First there is the issue of corporate responsibility. Incidents involving major Western-based high-tech firms and the dealing with repressive regimes around the globe[303] have made clear that businesses, driven by the market opportunities for Internet services and equipment, have all engaged in various forms of self-censorship of their services and have been less than forthcoming about the specific compromises they make in order to do business in countries that engage in censorship and surveillance.[304] Forcing these private entities to take responsibility and leading them to include human rights risk assessments in their decisions about market entry and product development could only be achieved by both private initiatives and legislative measures. The Global Network Initiative (GNI) represents such an initiative encouraging the development of collaborative strategies bringing together businesses, industry associations, civil society organizations, investors and academics in an effort to create and implement a code of conduct for free expression and privacy in the ICT sector.[305] It is important that Internet giants Yahoo, Google and Microsoft launched the initiative, now encouraging and inviting other companies especially those in the ICT sector to join the effort.[306]

However, as mentioned above, private initiative alone is not enough. Legislative measures should also be adopted especially by countries who export this technology. These measures could include provisions for legal support for the victims, establishing disincentive for private

corporations to collaborate with repressive surveillance and censorship, incentives for socially responsible technological development and measures to make collaboration with repression more difficult. The Global Online Freedom Act (GOFA)[307] aiming to prevent United States businesses from cooperating with repressive governments in Internet censorship and surveillance and to promote freedom of expression on the Internet would qualify as such a legislative piece. This bill was originally introduced in 2007, but it failed to gain traction in the U.S. House of Representatives. The bill was reintroduced in 2009.[308] GOFA would also create an Office of Global Internet Freedom at the State Department responsible for coordinating Internet freedom efforts and conducting research.[309] Other private initiates on specific matter have also surfaced during the last years.[310]

Additional action needs to be taken on a multi-national global level. It has been argued that Internet censorship should be considered a barrier to trade under the World Trade Organization.[311] In November the European think tank ECIPE asserted that WTO member states are "legally obliged to permit an unrestricted supply of cross-border Internet services."[312]

The ongoing battle between copyright holders and the end users is also unlikely to stop. As a matter of fact, as outlined above, it appears to get more aggressive. The regulation of piracy on an individual level has become an arms race between the entertainment industries stringent regulations and the hackers who defy the rules.[313] Phil Shiller, Senior Vice President of Worldwide Product Marketing at Apple, Inc. has indicated that the solution is not the continuous technical development of technologies to restrict access, but rather one of behavioral education.[314] Over the past several years social and cultural norms shifted to accept the concept of P2P file sharing as acceptable.[315] It is established that there are two fundamental reasons P2P file sharers partake in this behavior: 1) they do not have to behave and 2) they do not want to. The initial stringent approach taken by RIAA's user-directed litigation campaign provided for a major public relations issue for music distributors after such cases as *Capital Records v. Thomas* and *BMG Music Entertainment v. Tenenbaum*.[316] Rather than finding a decrease in file sharing, after the thousands of cases prosecuted by the RIAA, surveys indicate that P2P participants increased. P2P members began to perfect closed networks and encrypted file transfers.[317]

What is transparent is the need to educate the public of laws protecting intellectual property. WIPO and the Copyright Society of the USA (CSUSA) are beginning to provide targeted educational materials to teenagers and children.[318] WIPO currently offers a 75-page book directed at "young students", which provides basic information about copyrights and challenges presented in the technical age.[319] On the CSUSA website there is a section called "Copyright Kids!" which also teaches children from fifth through eighth grade of US copyright laws.[320] Ultimately, the positive reinforcement of education may prove to be a stronger deterrent in the future than the penal system previously used by the entertainment industry.

Taking into account the challenges described above, it is clear that there is no single right answer to the issue of protecting the freedom of expression online. It is however equally clear that a policy aimed at supporting global Internet freedom requires a sophisticated, multi-faceted, multi-sectoral, and truly global approach one that would bring together governments, companies and concerned citizens to find solutions to difficult new economic and security problems.

[1] *Reno v. Aclu*, 521 U.S. 844, 850-854 (U.S. 1997) where the Supreme Court provides an analysis of the Internet and its use. See also *Birth of the internet* providing a chronological map of the evolution of the Internet form the military network APRANET to today's web 0.2 available at http://www.cbc.ca/news/background/internet/(accessed May 27, 2010)

[2] This term was populized through the 1990s to refer to digital communication systems and the internet telecommunications network and is associated with United States Senator and later Vice-President Al Gore. See also Gregory Gromov,"Roads and Crossroads of Internet History" at http://www.netvalley.com/cgi-bin/intval/net_history.pl (accessed June 6, 2010).

[3] See Recommendations from the European Commission to the European Council: Europe and the Global Information Society (1994); First Annual Report of the Forum Information Society to the European Commission: Networks for People and their Communities. Making the Most of the Information Society in the European Union (1996); Resolution of the Council of Ministers, Nov. 21, 1996, 1996 O.J. (C 376) 1 (describing new policy-priorities regarding the information society); Interim Report from the High Level Expert Group on the Social and Societal Aspects of the Information Society: Building the European Information Society for Us All (1996). See also Al Gore, Bringing Information to the World: the Global Information Infrastructure, 9 Harv. J.L. & Tech. 1 (1996).

[4] , ACLU v. Reno, 929 F. Supp. 824, (E.D. Pa. 1996), aff'd, 521 U.S. 844 (1997).

[5] Id. at 881

[6] See infra Part III.

[7] See http://www.internetworldstats.com/stats.htm

[8] A traditional definition is the one Madison states: that the ability to transmit information through one's own person (free speech) or through the use of other material property (free press) needs special protection from government interference. See John O. McGinnis, The Once and Future Property- Based Vision of the First Amendment, 63 U. Chi. L. Rev. 49, 56-57 (1996). Later ,the concept was understood as being a social instrument in function of the democratic process: "The First Amendment does not protect a 'freedom to speak.' It protects the freedom of those activities of thought and communication by which we 'govern.'" Alexander Meiklejohn, The First Amendment is an Absolute, 1961 S. CT. Rev 245, 255. In Europe, the right to freedom of expression is interpreted as the right to seek, receive and impart information and ideas without interference by public authority and regardless of frontiers.

[9] See John O. McGinnis, The Once and Future Property- Based Vision of the First Amendment, 63 U. Chi. L. Rev. 49, 19 (1996). As early as 1996 the author noted that at that time the press was the (only) medium for publishing thoughts to a wide audience, whereas today, computer networks are fast becoming the most cost-effective way of delivering information. Id. at 100

[10] Broadcasting was subjected to specific free speech rules. See generally Thomas G. Krattenmaker & Lucas A. Powe, Jr., Converging First Amendment Principles for Converging Communications Media, 104 Yale L.J. 1719, 1721 (1995). See also Andreas Kohl, The International Aspects of the Freedom of Expression in Radio and Television, 8 Rev. Dr. H. 129 (1975); M. B<um u>llinger, Report on Freedom of Expression and Information: An Essential Element of Democracy, in Proceedings of the Sixth International Colloquy about the European Convention on Human Rights, 44, 86-126 (1985) available at : http://books.google.com/books?id=-3J_z-vs5qQC&pg=PA306&lpg=PA306&dq=Report+on+Freedom+of+Expression+and+Information:+An+Essential+Element+of+Democracy,+in+Proceedings+of+the+Sixth+International+Colloquy+about+the+European+Convention+on+Human+Rights&source=bl&ots=RheEY-Njyf&sig=cLQg_NyIzLKPot1obp-lA3EFHAM&hl=en&ei=s-X-S7qUM4_ANq20hTs&sa=X&oi=book_result&ct=result&resnum=1&ved=0CBMQ6AEwAA#v=onepage&q&f=false (accessed May 30, 2010).

[11] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." Amendment 1 of the United States Constitution". *The Bill of Rights: A Transcription*. 8601 Adelphi Road, College Park, MD 20740-6001: The U.S. National Archives and Records Administration at: http://www.archives.gov/exhibits/charters/print_friendly.html?page=bill_of_rights_transcript_content.html&title=The%20Bill%20of%20Rights%3A%20A%20Transcription. (accessed June 17, 2010)..

[12] The first amendment applies to the executive branch (e.g., *Bernstein v. U.S. Dept. of State*, 974 F Supp 1288 (ND Cal 1997)), and to the judicial branch (e.g., *Oregonian Pub. v. U.S. Dist. Court for Dist. of Or.*, 920 F2d 1462 (9th Cir 1990)). The clause is fully applicable to state and local governments through the Due Process Clause of the

Fourteenth Amendment. *44 Liquormart, Inc. v. Rhode Island*, 517 US 484, 116 S Ct 1495, 1501 n 1, 134 L Ed 2d 711 (1996).

[13] The European Union is a political and economic transnational organisation of European countries, characterized by a distribution of lawmaking powers between the Union and the Member States. Its legislative branch is composed of the European Commission, the European Council of Ministers and the European Parliament. The European Court of Justice is responsible for interpreting EU law and for resolving disputes concerning the interpretation of Community Treaties. See generally P. Kent, Law of the European Union 10-88 (1996); P.S.R.F. Mathijsen, A Guide to European Union Law (1995) and Christopher Harding & Ann Sherlock, European Community Law (1995).

[14] Koen Lenaerts, Fundamental Rights to be Included in a Community Catalogue, 16 Eur. L. Rev. 367, 371-372 (1991). This legal order has essentially a supervisory role, controlling the way in which member states comply with their ECHR obligations, but exercising no normative powers of its own. Id. See also Dirk Voorhoof, The Media in a Democratic Society, Legal Problems of the Functioning of Media in a Democratic Society 40-41 (Council of Europe ed. 1995) (describing the procedure in case of violation of the Convention by Member States). Still, the ECHR is a binding instrument for legislators of the Member States, as was explicitly confirmed in Article 1 of the Convention: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention." Supervision of the application of the ECHR is the responsibility of the organs of the European Convention: the European Commission of Human Rights, the Committee of Ministers and the European Court of Human Rights. Id.

[15] The European Commission of Human Rights at http://www.hri.org/docs/ECHR50.html#C.Art10 9ccessed June 15, 2010).

[16] Caroline Uyttendaele & Joseph Dumortier, FREE SPEECH ON THE INFORMATION SUPERHIGHWAY: EUROPEAN PERSPECTIVES, 16 J. Marshall J. Computer , &, Info. L. 905 (1998).

[17] *Roth v. United States*, 354 U.S. 476 (1957) "whether to the average person, applying contemporary community standards, the dominant theme of the material, taken as a whole, appeals to the prurient interest." *Miller v. California*, 413 U.S. 15 (1973). Under the *Miller* test, a work is obscene if: (a)...'the average person, applying contemporary community standards' would find the work, as a whole, appeals to the prurient interest,...(b)...the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c)...the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

[18] *Chaplinsky v. New Hampshire* (1942), "insulting or 'fighting words,' those that by their very utterance inflict injury or tend to incite an immediate breach of the peace" are among the "well-defined and narrowly limited classes of speech [which] the prevention and punishment of...have never been thought to raise any constitutional problem."

[19] *New York Times Co. v. Sullivan*.376 U.S. 254 (1964)

[20] See for instance 17 U.S.C. § 512

[21] Caroline Uyttendaele & Joseph Dumortier, FREE SPEECH ON THE INFORMATION SUPERHIGHWAY: EUROPEAN PERSPECTIVES, 16 J. Marshall J. Computer , &, Info. L. 905 (1998)

[22] The European Commission of Human Rights at http://www.hri.org/docs/ECHR50.html#C.Art10 9ccessed June 15, 2010).

[23] Caroline Uyttendaele & Joseph Dumortier, FREE SPEECH ON THE INFORMATION SUPERHIGHWAY: EUROPEAN PERSPECTIVES, 16 J. Marshall J. Computer , &, Info. L. 905 (1998)

[24] Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 Pepp. L. Rev. 427, 434 (2009).

[25] Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U.L. Rev. 1(2004).

[26] Id.

[27] Hannibal Travis, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law, 84 Notre Dame L. Rev. 331 (2009).

[28] Dawn C. Nunziato, The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115, 1122 (2005).

[29] The term "Web 2.0" was coined by eminent technologist and writer Tim O'Reilly. See Tim O'Reilly, What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, O'Reilly, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

[30] Hannibal Travis, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law, 84 Notre Dame L. Rev. 331 (2009).
[31] Id.
[32] Id.
[33] Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U.L. Rev. 1(2004).
[34] Id.
[35] Id.
[36] Id.
[37] Id.
[38] Id.
[39] Secretary Clinton: January 2010 » Remarks on Internet Freedom at http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed June 15, 2010) "Because amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. Just as steel can be used to build hospitals or machine guns, or nuclear power can either energize a city or destroy it, modern information networks and the technologies they support can be harnessed for good or for ill. The same networks that help organize movements for freedom also enable al-Qaida to spew hatred and incite violence against the innocent. And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights."
[40] Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U.L. Rev. 1(2004).
[41] Hannibal Travis, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law 84 Notre Dame L. Rev. 331 (2009).
[42] Id. See also infra Part III & IV.
[43] Lessig, Lawrence & Paul Resnick. "Zoning Internet Speech," 98 *Michigan Law Review* 395 (1999).
[44] Id. "For when viewed across jurisdictions, most controversial speech falls into category (3) — speech that is permitted to some in some places, but not to others in other places. What constitutes "political speech" in the United States (Nazi speech) is banned in Germany; 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.
[45] T.G.I. Paris, May 22, 2000, Gaz. Pal. 2000, somm. jurispr. 1307. An English translation is available Yahoo! Case Tribunal De Grande Instance De Paris May 22, 2000, Juriscom.net, at http://juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (last visited May 12, 2005)
[46] Id.
[47] Id.
[48] Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181, 1186, 1194 (N.D. Cal. 2001).
[49] Id. at 1193.
[50] Id. However, a Ninth Circuit panel overturned the district court's decision because the district court improperly asserted personal jurisdiction over the French parties. 379 F.3d 1120 (9th Cir. 2004). The Ninth Circuit has granted en banc review of the case. 399 F.3d 1010 (9th Cir. 2005).
[51] James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors, 66 U. Cin. L. Rev. 177 (1997).
[52] Id.
[53] For a short bio of John Gilmore see http://www.eff.org/about/board/ (accessed June 5, 2010)
[54] Electronic Frontier Foundation (EFF) ,founded in 1990 , is a non-profit organization dedicated to protecting defending free speech, privacy, innovation, and digital rights More information is vailable http://www.eff.org/about (accessed June 5, 2010).
[55] James Boyle, Foucault in Cyberspace, LECTURE: Foucault in Cyberspace +, 2 Yale Symp. L. , &, Tech. 2 (2000): "This tenet contains a vital technical truth. The Internet is a distributed network. It is a system which has no central node, no organizing exchange-no one single radio tower, broadcasting device, or control center. Thus it is extremely hard to shut down the Net. You put a blockage in one place, and messages flow like water around it. In

fact, "packet-switching" is basically a method of communication by hitchhiking. That is to say, when you write your e-mails or put together a web page, your data is broken up into several different packets, each carrying a little sign that says, "Going to New Haven." The packet of data then hitches a ride along the network. Some of the packets will travel by way of New York, some will travel by way of Boston, others will bounce around for ages until they finally get to their destinations where they will be integrated seamlessly. Try to imagine a censor trying to shut this thing down. It is like trying to grab the soap in the bath-you grab for it and it slips away. The idea of trying to exercise control over this seems impossible, hence the idea that the Internet treats censorship as a malfunction. The packets treat censorship the same way that they do a downed server-they just go around it."

[56] Id.

[57] Id.

[58] Id. citing John P. Barlow's , Selling Wine Without Bottles: The Economy of Mind on the Global Net, article in which he credits Stewart Brand with the statement.

[59] James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors, 66 U. Cin. L. Rev. 177, 182 (1997).

[60] Id.

[61] Id.

[62] Id.

[63] Reporters without Borders publish every year a list with the countries that regulate internet speech the most. This report is available at http://en.rsf.org/IMG/pdf/Internet_enemies.pdf (accessed May 25, 2010)

[64] *See, e.g.*, Pamela Samuelson, *Intellectual Property Issues Raised by the National Information Infrastructure*, 454 PLI/PAT 43 (1996).

[65] See generally Lawrence Lessig Code version .2, John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, 21 Wash. U. J.L. & Pol'y 31 (2006).

[66] See Prt II above. See also Nicholas P. Dickerson, THE THIRTEENTH ANNUAL FRANKEL LECTURE: COMMENT: WHAT MAKES THE INTERNET SO SPECIAL? AND WHY, WHERE, HOW, AND BY WHOM SHOULD ITS CONTENT BE REGULATED?,46 Hous. L. Rev. 61, 68-69 (2009).

[67] Id.

[68] Id.

[69] See generally Lawrence Lessig, Code: Version 2.0, at 44-45 (2006) (explaining end-to-end theory)

[70] See Lessig, supra note 37, at 44-45.

[71] Id.

[72] ACLU v. Reno (Reno I), 929 F. Supp. 824, 883 (E.D. Pa. 1996) (Dalzell, J., concurring).

[73] See John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to the End-to-End Principle, 21 Wash. U. J.L. & Pol'y 31, 36-37 (2006)

[74] See generally Jonathan Zittrain, Internet Points of Control, 44 B.C. L. Rev. 659 (2003).

[75] Id.

[76] 47 U.S.C. §223 (2000).

[77] 15 U.S.C. §7701 (2000); see also Derek E. Bambauer, Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising, 10 Va. J.L. & Tech. 5 (2005)

[78] See Jonathan Zittrain, Internet Points of Control, 44 B.C. L. Rev. 659, 671-672 (2003).

[79] Michael Geist, "The music industry's digital reversal," The Toronto Star, January 12, 2009. Available at: http://www.thestar.com/sciencetech/article/569203 (accessed May 28, 2010).

[80] 579 F. Supp. 2d 1210 (D. Minn. 2008).

[81] See Thomas, 579 F. Supp. 2d at 1226-27. The jury in the first trial returned a verdict against Thomas and awarded the plaintiffs statutory damages of $ 222,000 to compensate for twenty-four downloaded songs. The case was subsequently retried. In his decision granting Thomas's motion for a new trial based on an erroneous jury instruction, the judge himself said he thought the damages awarded were excessive, and he implored Congress to revisit the criteria for awarding large statutory damages in cases involving noncommercial infringement by individual consumers. See also Richard Koman, Wow! Jury Verdict in Capitol v. Thomas-Rasset: $ 2 Million, ZDNET, June 18, 2009, http://government.zdnet.com/?p=4990. Thomas's motion for a retrial was granted based on an error in the judge's jury instructions concerning whether the "making available" of music for download qualifies as distribution within the meaning of the Copyright Act.

[82] Capitol Records Inc. v. Thomas-Rasset, No. 06-1497 (MJD/RLE), 2010 U.S. Dist. LEXIS 504, at 1 (D. Minn. Jan. 22, 2010). at 2.
[83] see Tenenbaum, 2009 U.S. Dist. LEXIS 112845, at 2-3; see also 17 U.S.C. § 107 (2006).
[84] Student Ordered to Pay $ 675k for Downloads, CBS News, July 31, 2009, http://www.cbsnews.com/stories/2009/07/31/tech/main5203118.shtm (accessed June 6, 2010).
[85] David Kravets, Judge Finalizes $ 675,000 RIAA Piracy Verdict, Won't Gag Defendant, Wired, Dec. 7, 2009, http://www.wired.com/threatlevel/2009/12/piracy-verdict-finalized (accessed June 6, 2010).
[86] Genan Zilkha, The RIAA's Troubling Solution to File-Sharing, 20 Fordham Intell. Prop. Media , &, Ent. L.J. 667 (2010) Part I.B.

[87] Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," The Wall Street Journal, December 19, 2008. Available at: http://online.wsj.com/article/SB122966038836021137.html
[88] Mary Madden, Senior Research Specialist, The State of Music Online: Ten Years After Napster, Pew Internet & American Life Project, June 2009, pp 10-13. (accessed June 6, 2010).
[89] Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," The Wall Street Journal, December 19, 2008. Available at: http://online.wsj.com/article/SB122966038836021137.html (accessed June 6, 2010).
[90] 15 U.S.C. §§7704-05 (2000).
[91] . Id. §§6501-06.
[92] See OpenNet Initiative, Global Internet Filtering Map, http://map.opennet.net/ (identifying countries that partake in filtering on the internet);see also Reporters Sans Frontières - Web 2.0 versus Control 2.0 available at http://en.rsf.org/web-2-0-versus-control-2-0-18-03-2010,36697 (accessed June 6, 2010).; also Internet enemies and countries under surveillance at http://en.rsf.org/IMG/pdf/Internet_enemies.pdf (accessed June 6, 2010).
[93] John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, 21 Wash. U. J.L. & Pol'y 31 (2006).at 36-37 (noting the "tension between the desirability of the end-to-end principle and the desire to regulate certain behavior online").
[94] Need more citations re regulation of intermediaries Kathleen M. Sullivan & Gerald Gunther, Constitutional Law 1501 (15th ed. 2004).
[95] See Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 405 (2008).
[96] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.); 47 U.S.C. § 230(c)(1) (2000).
[97] See, e.g., Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (finding AOL not liable for defamatory statements published by one of its users); see also Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003) (holding GTE not liable after a user of one of its websites posted illegal videos of athletes changing in their locker room).
[98] 17 U.S.C. § 512(c)(1)(A)(iii) (2004).
[99] See 17 U.S.C. § 512(a) (2006); § 512. Limitations on liability relating to material online

(a) Transitory digital network communications. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if--

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

and injunctive relief against them must be limited to a court order requiring the termination of the Internet access of a subscriber or account holder adjudged to have engaged in infringing activity, or reasonable steps to block access from within the United States to a specific online location outside the United States adjudged to be infringing See id. id. § 512(j)(1)(B);

[100] Council Directive 2000/31, 2000 O.J. (L 178) 1 [hereinafter ECD].

[101] See id. art. 12, at 12.

[102] Id. art. 14, at 13.

[103] John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, 21 Wash. U. J.L. & Pol'y 31 (2006).at 31. See also generally Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, (2008)

[104] The Middle East and North Africa is one of the most heavily censored regions in the world.

[105] See genrally Code.2 http://en.rsf.org/IMG/pdf/Internet_enemies.pdf ; also THE THIRTEENTH ANNUAL FRANKEL LECTURE: COMMENT: WHAT MAKES THE INTERNET SO SPECIAL? AND WHY, WHERE, HOW, AND BY WHOM SHOULD ITS CONTENT BE REGULATED?*, 46 Hous. L. Rev. 61 (2009)

[106] Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed May 25, 2010).

[107] For more details on these filtering techniques, see Steven J. Murdoch and Ross Anderson, "Tools and Technology of Internet Filtering," Access Denied, (Cambridge: MIT Press, 2008), available at : http://opennet.net/sites/opennet.net/files/Deibert_04_Ch03_057-072.pdf . See also the OpenNet Initiative, "About Filtering," http://opennet.net/about-filtering (accessed May 25, 2010).

[108] Id.

[109] Id. See also United States v. Am. Library Ass'n, 539 U.S. 194 (U.S. 2003) (Stevens, J., dissenting : "Because of this "underblocking," the statute will provide parents with a false sense of security without really solving the problem that motivated its enactment. Conversely, the software's reliance on words to identify undesirable sites necessarily results in the blocking of thousands of pages that "contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions, such as 'pornography' or 'sex.'" Id., at 449. In my judgment, a statutory blunderbuss that mandates this vast amount of "overblocking" abridges the freedom of speech protected by the First Amendment).

[110] OpenNet Initiative, "About Filtering," http://opennet.net/about-filtering (accessed May 25, 2010). " Filtering based on dynamic content analysis—effectively reading the content of requested websites—though theoretically possible, has not been observed in our research"

[111] Id.

[112] Nart Villeneuve, The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace, First Monday, Jan. 4, 2006, http://firstmonday.org/issues/issue11 1/villeneuve/index.html.

[113] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008) citing Nart Villeneuve, The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace, First Monday, Jan. 4, 2006, http://firstmonday.org/issues/issue11 1/villeneuve/index.html (accessed June 6, 2010).

[114] See id.

[115] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

[116] See Jonathan Zittrain, Internet Points of Control, 44 B.C. L. Rev. 653 (2003).

[117] Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed June 6, 2010).

[118] See http://opennet.net/research/profiles/china#footnote6_tic8bin (accessed June 6, 2010).

[119] Google.cn presents to users a clear notification whenever links have been removed from our search results in response to local laws and regulations in China.2 – Google available at :

Schrage, E. (2006). "Testimony of Google Inc." *Joint Hearing of the Subcommittee on Africa, Global Human Rights & International Operations and the Subcommittee on Asia and the Pacific*. Retrieved, May 22 2008, from http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html (accessed June 6, 2010).

Where a government requests that we restrict search results, we will do so if required by applicable law and only in a way that impacts the results as narrowly as possible. If we are required to restrict search results, we will strive to achieve maximum transparency to the user. - Yahoo! available at :
Callahan, Michael. (2006). "Testimony of Michael Callahan." *Joint Hearing of the Subcommittee on Africa, Global Human Rights & International Operations and the Subcommittee on Asia and the Pacific*. Retrieved, May 22 2008, from http://yhoo.client.shareholder.com/releasedetail.cfm?releaseid=187725
When local laws require the company to block access to certain content, Microsoft will ensure that users know why that content was blocked, by notifying them that access has been limited due to a government restriction. – Microsoft available at : Krumholtz, J. (2006). "Congressional Testimony: The Internet in China: A Tool for Freedom or Suppression?" *Joint Hearing of the Subcommittee on Africa, Global Human Rights & International Operations and the Subcommittee on Asia and the Pacific*. Retrieved, May 22 2008, from http://www.microsoft.com/presspass/exec/krumholtz/02-15WrittenTestimony.mspx

[120] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

[121] Ronald Deibert, China's Cyberspace Control Strategy, February 2010, available at http://www.onlinecic.org/resourcece/archives/chinapapers (accessed June 5, 2010).

[122] Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, 2008, http://www.nartv.org/projects/search_monitor/searchmonitor.pdf (accessed June 6, 2010).

[123] Id.

[124] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

[125] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, at the University of Toronto, Canada focusing on advanced research and development at the intersection of digital media, global security, and human rights, http://citizenlab.org/ (accessed June 5, 2010).

[126] Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, 2008, http://www.nartv.org/projects/search_monitor/searchmonitor.pdf; also Ronald Deibert, China's Cyberspace Control Strategy, February 2010, available at *http://www.onlinecic.org/resourcece/archives/chinapapers* (accessed June 5, 2010).

[127] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008) citing Ronald Deibert, The Geopolitics of Asian Cyberspace, Far E. Econ. Rev., Dec. 2006, http://www.feer.com/articles1/2006/0612/free/p022.html

[128] Google and the threat to free speech - Times Online, available at : http://technology.timesonline.co.uk/tol/news/tech_and_web/article3634123.ece

[129] A new approach to China http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[130] A new approach to China http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[131] Id. See also Google to Stop Censoring Search Results in China After Hack Attack, Kim Zetter, available at: http://www.wired.com/threatlevel/2010/01/google-censorship-china/#ixzz0qvKA5zOI (accessed June 6, 2010).

[132] A new approach to China: an update, 3/22/2010 available at: http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[133] Nart Villeneuve, March 23, 2010 http://www.nartv.org/2010/03/23/google-cn-google-com-hk/

[134] Id.

[135] Lawrence Lessig, Code Version 2.0, at 39 (2006).

[136] OpenNet Initiative, A Starting Point: Legal Implications of Internet Filtering 5 (Sept. 2004), available at http://opennet.net/docs/Legal Implications.pdf.

[137] Bernhard Warner ,Google and the threat to free speech - Times Online March 27, 2008 available at : http://technology.timesonline.co.uk/tol/news/tech_and_web/article3634123.ece (accessed May 20, 2010); See also sami ben gharbia, Free Speech Roundup: Indonesia, Saudi Arabia, Turkey, Yemen available at : http://globalvoicesonline.org/2008/04/05/free-speech-roundup-indonesia-saudi-arabia-turkey-yemen/(accessed May 20, 2010).

[138] sami ben gharbia, Free Speech Roundup: Indonesia, Saudi Arabia, Turkey, Yemen available at : http://globalvoicesonline.org/2008/04/05/free-speech-roundup-indonesia-saudi-arabia-turkey-yemen/(accessed May 20, 2010).
[139] Bernhard Warner ,Google and the threat to free speech - Times Online March 27, 2008 available at : http://technology.timesonline.co.uk/tol/news/tech_and_web/article3634123.ece (accessed May 20, 2010).
[140] Id.

[141] BABAR DOGAR, Associated Press, *Pakistan lifts Facebook ban - Yahoo! News, May 31, 2010 available at* http://news.yahoo.com/s/ap/20100531/ap_on_re_as/as_pakistan_internet_crackdown (accessed June 5, 2010).

[142] Id. See also Facebook apologizes to Pakistan over 'sacrilegious' content available at http://www.siasat.pk/forum/showthread.php?36763-Facebook-Apologizes-to-Pakistan-IT-Ministry-Official&p=181185 (accessed June 6, 2010).
[143] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 412 (2008).
[144] See Human Rights in China, HRIC Case Highlight: Shi Tao and Yahoo, http://www.hrichina.org/public/highlight (summarizing Shi Tao's case) (accessed June 3, 2010); also Human Rights USA at http://www.humanrightsusa.org/index.php?option=com_content&task=view&id=15&Itemid=35 (accessed June 5, 2010).
[145] Changsha People's Procuratorate of Hunan Province v. Shi Tao (Changsha Interm. People's Ct. of Hunan Province, Apr. 27, 2005), translated in Case No. 19-10, at 29, http://www.globalvoicesonline.org/wp-content/ShiTao verdict.pdf In the judgment, it was revealed that Shi used his anonymous personal email account of huoyan-1989@yahoo.com.cn to send the notes. He identified himself as "198964." Id. at 29.
[146] Changsha People's Procuratorate of Hunan Province v. Shi Tao (Changsha Interm. People's Ct. of Hunan Province, Apr. 27, 2005), translated in Case No. 19-10, at 29, http://www.globalvoicesonline.org/wp-content/ShiTao verdict.pdf(accessed June 6, 2010).
[147] Changsha People's Procuratorate of Hunan Province v. Shi Tao, supra note 145 at 31.
[148] Id. at 28-29.
[149] Id. at 32.
[150] The Internet in China: A Tool for Freedom or Suppression?: Joint Hearing Before the Subcomm. on Africa, Global Human Rights and International Operations and the Subcomm. on Asia and the Pacific of the Comm. on International Relations, 109th Cong. 55, 58-59 (2006) [hereinafter Joint Hearing on the Internet in China] (statement of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc.), available at http://www.foreignaffairs.house.gov/archives/ 109/26075.pdf(accessed June 6, 2010).
[151] See also Statement of Chairman Lantos at hearing, Yahoo! Inc.'s Provision of False Information to Congress". http://www.internationalrelations.house.gov/press_display.asp?id=446 (accessed June 6, 2010).
[152] Testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., Before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific," U.S. House of Representatives Committee on International Relations, Joint Hearing: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, online at: http://www.nytimes.com/packages/pdf/business/YahooStatement.pdf (accessed June 6, 2010).
[153] Reporters Without Borders, Verdict in Cyberdissident Li Zhi Case Confirms Implication of Yahoo!, Feb. 27, 2006, http://www.rsf.org/article.php3?id article=16579 (accessed June 6, 2010).
See also http://www.humanrightsusa.org/index.php?option=com_content&task=view&id=15&Itemid=35
[154] Reporters Without Borders, Verdict in Cyberdissident Li Zhi Case Confirms Implication of Yahoo!, Feb. 27, 2006, http://www.rsf.org/article.php3?id article=16579. A Chinese version of the judgment is available at http://www.rsf.org/IMG/pdf/li zhi verdict.pdf. (accessed June 6, 2010).
[155] Shi Tao, Yahoo!, and the lessons for corporate social responsibility, Rebecca MacKinnon, online at http://rconversation.blogs.com/YahooShiTaoLessons.pdf (accessed June 6, 2010).
[156] Second Amended Complaint for Tort Damages at 14, Wang Xiaoning v. Yahoo! Inc., No. C07-02151 CW (N.D. Cal. July 30, 2007). The deprivation of political rights in China involves a fixed period of time after an individual is released from prison during which he or she is denied the rights of free speech and association granted to other

citizens. U.S. DEP'T OF STATE, BUREAU OF DEMOCRACY, HUMAN RIGHTS, AND LABOR, CHINA: COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES 2007 (2008), *available at* http://www.state.gov/g/drl/rls/hrrpt/2007/100518.htm (accessed June 6, 2010).
[157] Joint Stipulation of Dismissal at 1, Wang Xiaoning v. Yahoo! Inc., No. C07-02151 CW/JCS (N.D. Cal. Nov. 13, 2007). (accessed June 6, 2010).
[158] Seth Frinkelstein, Do You Have any Idea Who Last Looked at Your Data?, Guardian.co.uk, Nov. 15, 2007, http://www.guardian.co.uk/technology/2007/nov/15/comment. (accessed June 6, 2010).

[159] Jacqui Chen,Maybe a little evil: Google outs Indian man to authorities,at http://arstechnica.com/tech-policy/news/2008/05/maybe-a-little-evil-google-outs-indian-man-to-authorities.ars: see also Google and India Test the Limits of Liberty , Amol Sharma and Jessica E. Vascellaro at http://online.wsj.com/article/SB126239086161213013.html (accessed June 6, 2010).
[160] Id.

[161] Google Defends Helping Police Nab Defamer, By John Ribeiro, IDG News, http://www.pcworld.com/businesscenter/article/146049/google_defends_helping_police_nab_defamer.html (accessed June 16, 2010).

[162] Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 2006 U.S. Dist. LEXIS 49955 (N.D. Cal. 2006) Electronic Frontier Found., EFF's Case Against AT&T at http://www.eff.org/nsa/hepting (accessed June 5, 2010).
[163] Id.
[164] See Gonzales v. Google, Inc., 234 F.R.D. 674, 688 (N.D. Cal. 2006).
[165] Id. At 679

[166] Christopher Soghoian, 8 Million Reasons for Real Surveillance Oversight, December 1, 2009, at ://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (accessed June 14, 2010); also Kim Zetter ,Yahoo Issues Takedown Notice for Spying Price List, December 4, 2009 at http://www.wired.com/threatlevel/2009/12/yahoo-spy-prices/#ixzz0rDmlsB6l (accessed June 14, 2010).
[167] Id.
[168] Id. "I theorized that if I could obtain the price lists of each ISP, detailing the price for each kind of service, and invoices paid by the various parts of the Federal government, then I might be able to reverse engineer some approximate statistics."
[169] Id. Also http://files.cloudprivacy.net/verizon-price-list-letter.PDF (accessed June 20, 2010)
[170] I. See also http://files.cloudprivacy.net/yahoo-price-list-letter.PDF(accessed June 20, 2010)
[171] Available at http://www.google.com/governmentrequests/)

[172] Greater transparency around government requests David Drummond, SVP, Corporate Development and Chief Legal Officer at http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html (accessed June 16, 2010).
[173] See Government requests http://www.google.com/governmentrequests/faq.html
[174] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).
[175] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).
[176] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).
[177] Id.
[178] Id.
[179] Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).
[180]Jennifer A. Chandler, A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. 1095, 1117 (2007).

[181] *Search Engine Use*, Data Memo by Deborah Fallows, Senior Research Fellow, Pew Internet and American Life Project, August 6, 2008. At http://www.pewinternet.org/PPF/r/258/report_display.asp (accessed June 15, 2010).

[182] http://en-us.nielsen.com/rankings/insights/rankings/internet; see also http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=5

[183] Jennifer A. Chandler, A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. 1095, 1117 (2007) discussing Google's decision to remove the websites of BMW Germany and Ricoh Germany from its index because they had used banned methods to manipulate the search engine as well as the case of Search King, Inc. v. Google Technology, Inc. which dealt with a dispute over Google's ranking demotion of the plaintiff's website. Search King offered a match-making service designed to assist clients to buy and sell links from highly ranked websites in the hope of increasing the ranking of the linked-to websites. Google admitted that it had deliberately decreased the ranking of the Search King websites, stating that it was entitled to do so because Search King's actions undermined the integrity of its PageRank system while Search King argued that Google had demoted its websites because it was competing with Google, and sued for tortious interference with contractual relations. In Langdon v. Google, Inc., the plaintiff complained that Google would not let him purchase ads to advertise his websites, which criticized the North Carolina Attorney General (www.ncjusticefraud.com) and the Chinese government (www.chinaisevil.com). Google refused his anti-North Carolina Attorney General ad, citing its policy against advertisements that "advocate against an individual, group or organization" but failed to issue any decision regarding the plaintiff's short anti-China advertisement.

[184] See Andrew Goodman, Search Engine Showdown: Black Hats v. White Hats at SES, SearchEngineWatch, Feb. 17, 2005, http://searchenginewatch.com/showPage.html?page=3483941. (accessed June 15, 2010).

[185] Google writes: "Links help our crawlers find your site and can give your site greater visibility in our search results." Google Webmaster Help Center, How Can I Create a Google-friendly Site?, www.google.com/support/webmasters/bin/answer.py?answer=40349&topic=8522 (last visited Mar. 3, 2007).

[186] Google informs webmasters that "Google counts the number of votes a page receives as part of its PageRank assessment, interpreting a link from page A to page B as a vote by page A for page B. Votes cast by pages that are themselves "important' weigh more heavily and help to make other pages "important."' Id.

[187] Eric Goldman, Search Engine Bias and the Demise of Search Engine Utopianism, 8 Yale J.L. & Tech. 188, 189 (2006) (noting that search engines wield "significant power to shape searcher behavior and perceptions ... [and] the choices that search engines make about how to collect and present data can have significant social implications").

[188] Jennifer A. Chandler, A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. 1095 1117, (2007).

[189] A selection of recent papers includes Urs Gasser, Regulating Search Engines: Taking Stock and Looking Ahead, 8 Yale J.L. & Tech. 201, 208-16 (2006). (advocating a complete assessment of alternative regulatory approaches prior to deciding legislative intervention is the best solution); Goldman, supra note 45 (arguing that search engine bias is necessary and desirable, and that regulatory intervention is unwarranted); Frank Pasquale, Rankings, Reductionism, and Responsibility, 54 Clev. St. L. Rev. 115, 135-39 (2006) (proposing legal remedies for harms claimed to flow from unwanted inclusion or exclusion in search engine results); Andrew Sinclair, Note, Regulation of Paid Listings in Internet Search Engines: A Proposal for FTC Action, 10 B.U. J. Sci. & Tech. L. 353, 364-66 (2004) (advocating, among other things, FTC action against search engines that use paid listings without disclosing this fact to consumers).

[190] Introna & Nissenbaum, supra note 7, at 61; Gasser, supra note 41, at 232-34.

[191] Gasser, supra note 189 at 233.

[192] Gasser, supra note 189, at 233-34.

[193] America Online, Agreement to Rules of User Conduct, at http://www.aol.com/copyright/rules.html (accessed June 15, 2010).

[194] Id.

[195] Yahoo!, Terms of Service, at http://docs.yahoo.com/info/terms (accessed June 15, 2010).

[196] Id. Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115 (2005)

[197] Comcast Cable Communications, LLC, Comcast High-Speed Internet Acceptable Use Policy, at http://www.comcast.net/terms/use.jsp (accessed June 15, 2010).

[198] Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115 (2005)1120-1123. The author also discusses how Colleges and universities, both private and public, also serve as Internet access providers for millions of students across the United States have established and enforced "acceptable use policies" that substantially restrict First Amendment protected speech.aas well as private employers, which serve as Internet access providers for millions of employees across the United States, routinely monitor and restrict e-mail (and Internet use generally), with approximately 50-60% of employers monitoring e-mail.

[199] Chris Sogohian, Google censors political-donation transparency ads, December 17, 2008 at http://news.cnet.com/8301-13739_3-10122713-46.html (accessed June 10, 2010).

[200]Id.

[201] Sherriff, Lucy (21 September 2006). "Google erases Operation Ore campaign site". The Register. http://www.theregister.co.uk/2006/09/21/google_delists_inq21/.(accessed June 15, 2010).

[202] Christopher Landau Google climbdown on abortion ads, 17 September 2008 http://news.bbc.co.uk/2/hi/uk_news/7621751.stm (accessed June 15, 2010).

[203] Dawn Nunziato The Death of the Public Forum in Cyberspace,20 Berkeley Tech. L.J. 1115, 1124-1125 (2005)
[204] Id. at n.28.
[205] Barbara van Schewick, Towards an Economic Framework for Network Neutrality Regulation, 5 J. Telecomm. & High Tech. L. 329, 336 (2007)
[206] Benjamin Rupert, The 110th Congress and Network Neutrality: S. 215 - The Internet Freedom Preservation Act, 18 DePaul J. Art, Tech. & Int'l Intell. Prop. L. 325, 240-41 (2008).
[207] Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115, 1123 (2005)
[208] Don Marti, "Google Begins Making DMCA Takedowns Public," *Linux Journal* (2002/4/12) (describing Google's response to the Scientologists and subsequent decision to contribute to ChillingEffects.org). Gallagher, David F. (2002-04-22). http://www.linuxjournal.com/article/5997 (accessed June 15, 2010); "New Economy; A copyright dispute with the Church of Scientology is forcing Google to do some creative linking". New York Times. http://query.nytimes.com/gst/fullpage.html?res=9F02E5D7103FF931A15757C0A9649C8B63&sec=&spon=&page wanted=all. (accessed May 29, 2010).

[209] "Google Somewhat Lifts Oceana Ad Ban". webpronews.com. 2004-05-17(accessed June 10, 2010). http://www.webpronews.com/topnews/2004/05/17/google-somewhat-lifts-oceana-ad-ban.The policy was later changed
[210] See Brian Stelter, To Curb Traffic on the Internet, Access Providers Consider Charging by the Gigabyte, N.Y. Times, June 15, 2008, at A1, available at http://www.nytimes.com/2008/06/15/technology/15cable.html?pagewanted=1 (accessed June 15, 2010).
[211] Id.

[212] EFF Test Your ISP https://www.eff.org/testyourisp (accessed June 15, 2010).: "In specific, Comcast was injecting forged RST packets into TCP communications, in an effort to disrupt certain protocols commonly used for file-sharing. The interference efforts were triggered by the protocol that the subscriber used, not by the number of connections made or amount of bandwidth used by the subscriber.
[213] Peter Eckersley, Fred von Lohmann and Seth Schoen November 28, 2007http://www.eff.org/files/eff_comcast_report2.pdf(accessed June 15, 2010). ; see also In re Free Press & Pub. Knowledge, 23 F.C.C.R. 13028, 13031 (2008) (describing the AP study). Comcast argued that it was merely slowing and not actually blocking P2P traffic, but the Federal Communications Commission found otherwise. See id. at 13053-54 (finding that "whether or not blocking was Comcast's intent, Comcast's actions certainly had that effect in some circumstances").
[214] Comcast Corp. v FCC, No. 08-1291 (D.C. Cir., Apr. 6, 2010) Full text of opinion available at : http://pacer.cadc.uscourts.gov/common/opinions/201004/08-1291-1238302.pdf (accessed June 15, 2010).

[215] Tyler Lacey April 11, 2010 Comcast Corp. v. FCC D.C. Circuit Denies FCC Jurisdiction to Mandate Net Neutrality http://jolt.law.harvard.edu/digest/telecommunications/comcast-corp-v-fcc; also Stacey Higginbotham,

Comcast vs FCC: In Battle For Net Neutrality, Did the Courts Hand Comcast a Pyrrhic Victory? April 6, 2010 at: http://gigaom.com/2010/04/06/did-the-courts-hand-comcast-a-pyrrhic-victory/(accessed June 15, 2010).

[216] Bloomberg Businessweek, Comcast Wins in Case on FCC Net Neutrality Powers (update 6) http://www.businessweek.com/news/2010-04-06/comcast-wins-in-case-on-fcc-net-neutrality-powers-update6-.html (June 4, 2010)

[217] Paul Barbagallo, FCC Broadband Proposal Faces New Scrutiny, With Over 240 House Members Now Opposed , June 2, 2010 http://news.bna.com/pwdm/PWDMWB/split_display.adp?fedfid=17261986&vname=prabulallissues&wsn=499750500&searchid=11543456&doctypeid=1&type=date&mode=doc&split=0&scm=PWDMWB&pg=0 (subscription required) (accessed June 15, 2010).; also *Fred von Lohmann*, Court Rejects FCC Authority Over the Internet, April 6, 2010, at : https://www.eff.org/deeplinks/2010/04/court-rejects-fcc-authority-over-internet (accessed June 15, 2010).

[218] Brett M. Frischmann & Barbara van Schewick, Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo, 47 Jurimetrics J. 383, 387-89 (2007). See also Milton Mueller Net Neutrality as Global Norm for Internet Governance at http://www.internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf (accessed June 15, 2010).

[219] See Lawrence Lessig, The Future Of Ideas 46-48, 155-76, 246-49 (2002)

[220] See, also Adam Liptak, Verizon Rejects Text Messages from an Abortion Rights Group, N.Y. Times, Sept. 27, 2007, at A1 (citation omitted); Adam Liptak, Verizon Reverses Itself on Abortion Messages, N.Y. Times, Sept. 28, 2007, available at http://www.nytimes.com/2007/09/28/business/28verizon.html. (accessed June 15, 2010).

[221] Jack M. Balkin, FREE SPEECH AND PRESS IN THE DIGITAL AGE: THE FUTURE OF FREE EXPRESSION IN A DIGITAL AGE, 36 Pepp. L. Rev. 427, 444 (2009)

[222] Barbara van Schewick, Towards an Economic Framework for Network Neutrality Regulation, 5 J. Telecomm. & High Tech. L. 329, 336 (2007)

[223] See Peter Svensson, Comcast Blocks Some Internet Traffic, S.F. Chron., Oct. 19, 2007, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/10/19/financial/f061526D54.DTL&feed=rss.business. (accessed June 15, 2010).

[224] Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181, 1186, 1194 (N.D. Cal. 2001).

[225] See Lori Enos, Yahoo! To Ban Nazi-Related Auctions, E-Commerce Times, Jan. 3, 2001, available at http://www.ecommencetimes.com/story/6432.html. (accessed June 15, 2010).

[226] Alexander Tsesis, Hate in Cyberspace: Regulating Hate Speech on the Internet, 38 San Diego L. Rev. 817, 866 (2001).

[227] Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115 (2005)

[228] Jack M. Balkin, FREE SPEECH AND PRESS IN THE DIGITAL AGE: THE FUTURE OF FREE EXPRESSION IN A DIGITAL AGE, 36 Pepp. L. Rev. 427 (2009)

[229] Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 Pepp. L. Rev. 16 (2009)

[230] See above Part II.

[231] 17 U.S.C. 512(h). Doris E. Long , ELECTRONIC VOTING RIGHTS AND THE DMCA: ANOTHER BLAST FROM THE DIGITAL PIRATES OR A FINAL WAKE UP CALL FOR REFORM?" 23 J. Marshall J. Computer & Info. L. 533, 535-540

[232] Id. "To obtain the subpoena, the copyright owner is only required to provide a written notice that includes the following: (1) a clear identification of the copyrighted work allegedly being infringed; (2) a clear identification of the alleged infringing material; (3) "reasonably sufficient" information that will allow the ISP to locate the material at issue; (4) a statement of good faith belief the work is being infringed; and (5) a declaration that the identity of the subscriber in question will only be used for the purpose of protecting the owner's copyright."

[233] 17 U.S.C. 512(c).

[234] 17 U.S.C. 512(h)(5)

[235] Id.

[236] Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003)

[237] See id. at 1237.
[238] see also John Borland, Court: RIAA Lawsuit Strategy Illegal, CNET News, Dec. 19, 2003, http://news.cnet.com/2100-1027_3-5129687.html [hereinafter Borland, RIAA Lawsuit]. Before the Verizon decision came down, the RIAA had already issued more than 3,000 subpoenas. Electronic Frontier Found., RIAA v. The People: Four Years Later 5 (2007), available at http://w2.eff.org/IP/P2P/riaa_at_four.pdf. Users who received this subpoena included a twelve-year-old girl living in a housing project in New York City, and a grandmother, whom, it was later discovered, had been wrongfully accused. Id. at 4. The accused were given the opportunity to settle or go to trial. Id. The majority of users settled for around $ 3,000. Id. One user who refused to settle faced a $ 22,500 judgment. Bob Mehr, Gnat, Meet Cannon: Cecila Gonzalez Doesn't Want to Fight the Recording Industry. She Doesn't Have a Choice, Chi. Reader, Feb. 3, 2005, http://www.chicago reader.com/chicago/gnat-meet-cannon/Content?oid=917905. (accessed June 15, 2010).
[239] Treacy, Bridget, *Data Protection Law & Policy*, 5 (March 2008).
[240] Case C-275/06, Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU (Telefonica), 2008 E.C.R. 1-00271, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0275:EN:HTML. (accessed June 15, 2010).
[241] Id.
[242] Id.
[243] *Id*..
[244] *Id*.
[245] *Id*.
[246] Id. see also Treacy, Bridget, *Data Protection Law & Policy*, 5-6 (March 2008).
[247] See infra . see also Eliot Van Buskirk, RIAA to Stop Suing Music Fans, Cut Them Off Instead, Wired, Dec. 19, 2008, http://blog.wired.com/business/2008/12/riaa-says-it-pl.html; Mathew Ingram, RIAA Drops Lawsuit Strategy for "Three Strikes" Plan, Gigaom, Dec. 19, 2008, http://gigaom.com/2008/12/19/riaa-drops-lawsuit-strategy-for-three-strikes-plan; Nate Anderson, RIAA Graduated Response Plan: Q&A with Cary Sherman, Ars Technica, Dec. 21, 2008, http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars. (accessed June 15, 2010).
[248] Mathew Ingram, RIAA Drops Lawsuit Strategy for "Three Strikes" Plan, Gigaom, Dec. 19, 2008, http://gigaom.com/2008/12/19/riaa-drops-lawsuit-strategy-for-three-strikes-plan. (accessed June 15, 2010).
[249] Nate Anderson, RIAA Graduated Response Plan: Q&A with Cary Sherman, Ars Technica, Dec. 21, 2008, http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars. (accessed June 15, 2010).
[250] Mathew Ingram, RIAA Drops Lawsuit Strategy for "Three Strikes" Plan, Gigaom, Dec. 19, 2008, http://gigaom.com/2008/12/19/riaa-drops-lawsuit-strategy-for-three-strikes-plan. (accessed June 15, 2010).

[251] See id.
[252] See id.

[253] See Andrew Lyle, RIAA to Stop Suing Users, Cuts Them Off Instead, Neowin, Dec. 19, 2008, http://www.neowin.net/news/main/08/12/19/riaa-to-stop-suing-users-cuts-them-off-instead. See also Karl Bode, AT&T Wants Government Website Blacklists, Hadopi-Style Tribunal, May 3, 2010 at http://www.techdirt.com/articles/20100430/1423539264.shtml (accessed June 15, 2010).
[254] 17 U.S.C. § 512(j)(1)(A)(ii) (2006).
[255] See id.
[256] See id
[257] See id.
[258] Jennifer M. Urban & Laura Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 639 (2006).
[259] Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010).

[260] la Rédaction de Net-iris et publié le vendredi 15 mai 2009.Les missions de la Haute Autorité pour la diffusion des oeuvres et la protection des droits sur internet at : http://www.net-iris.fr/veille-juridique/actualite/22267/les-missions-de-la-haute-autorite-pour-la-diffusion-des-oeuvres-et-la-protection-des-droits-sur-internet.php(accessed June 15, 2010).

[261] Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010).
[262] Id. see also "Hadopi: le Conseil constitutionnel censure la riposte graduée" (in French). *Le Monde*. 10 June 2009. http://www.lemonde.fr/technologies/article/2009/06/10/hadopi-le-conseil-constitutionnel-censure-la-riposte-graduee_1205290_651865.html. (accessed June 15, 2010).
[263] Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010). " […] HADOPI 2 provides that a single judge may render a decision without informing the pirate and without any debate between the parties. However, as soon as the "pirate" receives the judge's decision, they may challenge this decision within 45 days, following which a traditional procedure shall be followed, in which the web user may defend their case."
[264] Full text of the Act as amended and put into force available at "http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=3699621(accessed June 15, 2010).
[265] "Controversial UK anti-piracy law finally passed". Telecoms Europe. http://www.telecomseurope.net/content/controversial-uk-anti-piracy-law-finally-passed?section=HEADLINE&utm_source=lyris&utm_medium=newsletter&utm_campaign=telecomseurope. Retrieved 9 April 2010.
[266] Full text of the Act as amended and put into force available at "http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=3699621(accessed June 15, 2010).
Clause 18 on "Preventing access to specified online locations for the prevention of online copyright infringement".

[267] Id. see also Charles Arthur Digital economy bill: what you need to know, Mach 22, 2010 at : http://www.guardian.co.uk/media/2010/mar/22/digital-economy-bill
[268] See *By* Ali Qassim *april 2010*. http://news.bna.com/pwdm/PWDMWB/split_display.adp?fedfid=16980236&vname=prabulallissues&wsn=499955500&searchid=11543456&doctypeid=1&type=date&mode=doc&split=0&scm=PWDMWB&pg=0 (subscription required)(accessed June 15, 2010).

[269] see e.g open rights group Jim Killock, Digital Economy Bill: dangerous and draconian just got dictatorial

20 November 2009 http://www.openrightsgroup.org/blog/2009/digital-economy-bill; David Meyer, Open Wi-Fi 'outlawed' by Digital Economy Bill(accessed June 15, 2010).

ZDNet UK, 26 February, 2010 at : http://www.zdnet.co.uk/news/networking/2010/02/26/open-wi-fi-outlawed-by-digital-economy-bill-40057470/(accessed June 15, 2010).
[270] UK Politicians Looking To Repeal Digital Economy Act
from the *good-for-them* dept at Http://www.techdirt.com/articles/20100518/0900499464.shtml(accessed June 15, 2010).

[271] Mike Mesnick New Zealand Copyright Minister Sneaks In 3 Strikes Law; Yells At Those Who Ask Why, Oct 10th 2008at http://www.techdirt.com/articles/20081009/2144022508.shtml(accessed June 15, 2010).

[272] Mike Mesnick, New Zealand Moves Forward With Three Strikes; Big Questions Left Unanswered April 10 , 2010 at: http://www.techdirt.com/articles/20100425/2121239163.shtml; see also NZPA Three strikes for online copyright abusers February 26, 2010 at : http://tvnz.co.nz/technology-news/three-strikes-online-copyright-abusers-3383024(accessed June 15, 2010).

[273] Four strikes in the Belgium draft copy of the French Hadopi law, 24 March, 2010 at: http://www.edri.org/edrigram/number8.6/four-strikes-belgium(accessed June 15, 2010).

[274] see generally Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009).
[275] Genan Zilkha, Note: The RIAA's Troubling Solution to File-Sharing, 20 Fordham Intell. Prop. Media , &, Ent. L.J. 667 , 701 (2010).
[276] Greg Sandoval, AT&T First to Test RIAA Antipiracy Plan, CNET News, Mar. 24, 2009, http://news.cnet.com/8301-1023_3-10203799-93.html?tag=mncol;txt. (accessed June 15, 2010).
[277] Verizon, Support, Announcements, https://www.verizon.net/central/vzc.portal?_ nfpb=true&_pageLabel=vzc_help_announce ment&id=copyright (last visited Jan. 4, 2009). (accessed June 15, 2010).
[278] Id. David Carnoy, Verizon Ends Service of Alleged Illegal Downloaders, CNET News, Jan. 20, 2010, http://news.cnet.com/8301-1023_3-10437176-93.html.
[279]

[280] David Carnoy, Verizon Ends Service of Alleged Illegal Downloaders, CNET News, Jan. 20, 2010, http://news.cnet.com/8301-1023_3-10437176-93.html.
[281] Amol Rajan, *Virgin Warns Illegal Downloaders: Stop or Face Prosecution*, THE INDEP., June 7, 2008, http://www.independent.co.uk/arts-entertainment/music/news/virgin-warns-illegal-downloaders-stop-or-face-prosecution-842086.html. (accessed June 15, 2010).

[282] Lars Brandle, *ISPs On The Agenda At BPI AGM*, BILLBOARD.BIZ, July 9, 2008, http://www.billboard.biz/bbbiz/content_display/industry/e3i3a02b4b8960ca28a1cbaf4bafed07503. (accessed June 15, 2010).
[283] Press Release, U.K., Dept. for Bus., Enter. & Reg. Reform, New Measures to Address Online File-Sharing (July 24, 2008), http://www.wired-gov.net/wg/wg-news-1-nsf/0/788A1BAE10F752DB80257 490002B4756?OpenDocument. (accessed June 15, 2010).

[284] *Net Firms in Music Pirates Deal*, BBC NEWS, July 24, 2008, http://news.bbc.co.uk/2/hi/technology/7522334.stm.>ENDFN> (accessed June 15, 2010).

[285] JOHN COLLINS, Eircom to cut broadband over illegal downloads, , May 24, 2010, at http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html (accessed June 15, 2010).

[286] JOHNNY Ryan, Three strikes, copyright and copytight? 24 April 2010 At http://johnnyryan.wordpress.com/2010/04/24/three-strikes-copyright-and-copytight/ (accessed June 15, 2010). "A case in the Irish High Court between Eircom and the Irish Recorded Music Association (IRMA) resulted in a settlement in January 2009. Under the agreement Eircom has committed to:

1. inform its broadband subscriber that the subscriber's IP address has been detected infringing copyright and
2. warn the subscriber that unless the infringement ceases the subscriber will be disconnected and
3. in default of compliance by the subscriber with the warning it will disconnect the subscriber."

[287] JOHN COLLINS, Eircom to cut broadband over illegal downloads, , May 24, 2010, at http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html(accessed June 15, 2010).; see also Irish ISP Launches a Voluntary "Three-Strikes" Policy, May 26th, 2010 http://extratorrent.com/article/511/irish+isp+launches+a+voluntary+%E2%80%9Cthree+strikes%E2%80%9D+policy.html(accessed June 15, 2010).

[288] For a detailed analysis of the benefits nad drawbacks of the graduated response scheme see Yu, Peter K., The Graduated Response (March 28, 2010). Florida Law Review, Vol. 62, 2010. Available at SSRN: http://ssrn.com/abstract=1579782.; see also Genan Zilkha, Note: The RIAA's Troubling Solution to File-Sharing, 20 Fordham Intell. Prop. Media , &, Ent. L.J. 667 (2010). "In a study by the University of Washington, three computer scientists found that the RIAA method of tracking illegal file-sharers and sending them takedown notices was unreliable and "inconclusive." These scientists were able to convince the RIAA through manipulations that machines that were not sharing files actually were sharing files. The scientists also found that while some users were caught even though they were not doing anything illegal, other users could intentionally avoid being tracked. For example, the Pirate Bay, a widely used BitTorrent tracker, has offered a virtual private network ("VPN") subscription service, called IPREDator, that claims to mask IP addresses of subscribers so that they can escape RIAA detection. The University of Washington scientists further found that "it is possible for a malicious user (buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials." A study by Google found that 57% of takedown notices it received under the DMCA were sent by business competitors who were trying to undercut each other, and that 37% of notices were "not valid copyright claims." The RIAA has even admitted that it has sent out mistaken takedown notices in the past. In a particularly embarrassing case, the RIAA sent a takedown notice to Penn State University, stating that someone in the "astronomy and astrophysics department had illegally uploaded songs by the artist [Usher] for free distribution" based on the existence of a file entitled "Usher." In reality, the file was an a cappella song uploaded by Professor Usher. After apologizing, the RIAA admitted that it had "sent out dozens of mistaken notices in the past, and at times, did not always fully confirm a suspected case of infringement." Faulty methodology thus undermines the strength of the RIAA's claims.

[289] Peter K.,Yu The Graduated Response (March 28, 2010). Florida Law Review, Vol. 62, 2010. Available at SSRN: http://ssrn.com/abstract=1579782, pp 15-17. (accessed June 15, 2010).

[290] Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010).

[291] Swedish BitTorrent tracker the Pirate Bay available at : http://thepiratebay.org/(accessed June 15, 2010).

[292] See IP Redator at: https://www.ipredator.se/?lang=en(accessed June 15, 2010).

[293]Martyn Warwick TelecomTV: the Foolishness of Hadopi 2, the French Internet Law, march 16, 2010 at http://www.mediafuturist.com/2010/03/foolishness-of-hadopi-2.html(accessed June 15, 2010).

[294] Id.

[295] Peter K.,Yu The Graduated Response (March 28, 2010). Florida Law Review, Vol. 62, 2010. Available at SSRN: http://ssrn.com/abstract=1579782, p 4. (accessed June 15, 2010).

[296] Michael Geist, Australian Judge Explains Why Three Strikes Isn't Reasonable, February 03, 2010 at: http://www.michaelgeist.ca/content/view/4760/125/(accessed June 15, 2010).

[297] Press Release, Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens, 5 November 2009 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491

[298] Id. see also A "FAQs on internet access safeguards and the telecoms package" document released Nov. 5 by negotiators is available at http://www.europarl.europa.eu/pdfs/news/expert/background/20091105BKG63887/20091105BKG63887_en.pdf. (accessed June 15, 2010).

Further information on the new agreement, including the archived webcast of the press conference announcing the compromise package, is available at http://www.se2009.eu/en/meetings_news/2009/11/5/europe_united_on_telecoms_package?localLinksEnabled=false (accessed June 15, 2010).

[299] Press Release, Anti-Counterfeiting Trade Agreement: European Commission welcomes release of negotiation documents 21 April 2010 http://trade.ec.europa.eu/doclib/press/index.cfm?id=552; see also David Meyer, Europe "Will Not Accept" Three Strikes in ACTA Treaty, ZDNET, Feb. 26, 2010, http://news.zdnet.co.uk/communications/0,1000000085,40057434,00.htm. *(accessed June 15, 2010).*

[300] Secretary Clinton: January 2010 » Remarks on Internet Freedom at http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed June 15, 2010)

[301] Id.

[302] Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed June 15, 2010)

[303] Id. see also part III.

[304] See Ronald Deibert, China's Cyberspace Control Strategy, February 2010,discussing the case of "a recently leaked Cisco presentation from 2002 showing that company members viewed China's then emerging censorship system (the so-called "Golden Shield") as a market opportunity, thus contradicting repeated claims made by the company that it is not morally responsible for sales of its equipment to regimes that censor and engage in surveillance" available at http://www.onlinecic.org/resourcece/archives/chinapapers (accessed June 5, 2010).

[305] See Global Network Initiative at http://www.globalnetworkinitiative.org/corecommitments/index.php (accessed June 10, 2010).

[306] Id. see also Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed June 15, 2010)

[307] H.R. 2271: Global Online Freedom Act of 2009, at http://www.govtrack.us/congress/bill.xpd?bill=h111-2271 (accessed June 5, 2010).

[308] See also Bobbie Johnson Obama urged to punish US firms for aiding internet censorship 30 June 2009 at http://www.guardian.co.uk/world/2009/jun/30/us-firms-aiding-censorship (accessed June 15, 2010).

[309] Roy Mark, Google China Dispute Revive Global Online Freeedom Act, January, 17, 2010 at http://www.eweek.com/c/a/Government-IT/Google-China-Dispute-Revives-Global-Online-Freedom-Act-493296/(accessed June 15, 2010)

[310] Civil liberties group The Electronic Frontier Foundation along with Google and numerous other public interest organizations and Internet industry associations have joined with Yahoo in asking a federal court to block a government attempt to access a Yahoo! email account based on probable cause without a search warrant. Joins With Google and Others to Argue for Fourth Amendment Protection of Email at https://www.eff.org/press/archives/2010/04/13 (accessed June 15, 2010). See also EFF Joins With Internet Companies and Advocacy Groups to Reform Privacy Law Coalition Urges Updates to Electronic Privacy Statute to Reflect Web 2.0 World, March 3, 2010 at http://www.eff.org/press/archives/2010/03/30 (accessed June 15, 2010)

[311] Id.

[312] Brian Hindley and Hosuk Lee-Makiyama "Protectionism Online: Internet Censorship and International Trade Law, ECIPE Working Paper No. 12/2009, at: http://www.ecipe.org/protectionism-online-internet-censorship-and-international-trade-law/PDF (accessed June 15, 2010)

[313] Annemarie Bridy, WHY PIRATES (STILL) WON'T BEHAVE: REGULATING P2P IN THE DECADE AFTER NAPSTER, 40 Rutgers L.J. 565, 570 (2009)
[314] *Id*. at 600
[315] *Id*. at 601.
[316] *Id*. at 603.
[317] *Id*. at 609.
[318] *Id*. at 605.
[319] *Id*.
[320] *Id*. at 606.