The fine balance between security and fundamental rights — the (proposal) of the Brazilian Bill of "Civil Rights Framework for Internet"

Jorge Machado[1]

Alcimar Queiroz[2]

Research Group on Public Policies for Access to Information (GPOPAI)

University of São Paulo, Brazil

(2010)

Presented at Workshop **World Internet Policy Project** (WIP2)

Lisboa. Portugal, 2010

Abstract:

The Brazilian Ministry of Justice started an initiative for the establishment of a civil-rights based legal framework for the use of the Internet. The main goal is to structure rights and responsibilities for using the web, as well as the conditions to provide access to private data. This law is expected to help solve conflicts related to privacy and freedom of expression in Internet by guaranteeing fundamental rights, as opposed to criminalizing or restricting rights.

Keywords:

Internet; Regulatory Aspects; Civil Rights; Privacy; Freedom of Expression.

---

1 Professor of School of Arts, Sciences and Humanities (EACH), University of São Paulo. Graduate in Social Sciences from the University of São Paulo (1996), Ph.D. in Sociology from the University of Granada, Spain (2001) and post-doctorate at the University of Campinas, Brazil (2004). Conducts research in the GPOPAI (Research Group on Public Policies for Access to Information). Works in Public Policy, mainly in the following themes: policies for access to information, political science, information technology, right to information and collaborative production of knowledge. Contact: machado@usp.br

2 Ph.D. Candidate in Sociology at Higher Institute of Business and Labour Sciences (ISCTE-Portugal), and in Education at Faculty of Education of University of São Paulo - Brasil. Graduated in Pedagogy (2001) from University of São Paulo, from where he also got a Masters Degree in Sociology of Education (2005). He researches on the relationships of Human Rights and Information Society in the Iberian-American countries at LINI (Lisbon Internet and Networks Institute) and GPOPAI (Research Group on Public Policies for Access to Information). Contact: asqz@usp.br

1. Introduction

The behaviour of Internet users is sometimes incongruent with the law, mainly because the legislation is inappropriate for the social practices, techniques and demands of the internet users. As a result , the judiciary has made controversial decisions in Brazil, as well as in other countries that directly or indirectly affect fundamental rights, as we will show below.

The Brazilian Ministry of Justice recently developed a collaborative process for the establishment of a civil rights based legal framework for the use of the Internet[3]. The main goal is to structure rights and responsibilities for using the web, as well as providing access and contents (Marco Civil, 2010). The idea is to regulate conflicts related to privacy and freedom of expression on the Internet not by criminalizing or restricting the rights, but rather by guaranteeing fundamental rights established by the Constitution.

This debate was structured in two 45-day phases. The first phase (finished on December 17th) was based on the selection of key issues such as privacy, freedom of expression, network neutrality, storage of logs, legal responsibilities and Government guidelines. During this period, the Public consultation benefited from more than 822 contributions from civil society as well as official reports by important institutions on the matter. The second phase – from April 8th to 23rd May 2010 - began with the publication of the complete draft of the bill. This phase obtained 1,168 contributions from different groups, associations, agencies, and scholars. The final document is expected to be submitted to the National Congress on July 2010.

3 This project is developed in a partnership between the Ministry of Justice of Brazil with the Center for Technology and Society from Fundação Getúlio Vargas (FGV/CTS).

In many countries, Internet regulations are being pressured with proposals to tighten censorship and control, disregarding privacy and citizen's rights. The Brazilian Government proposal considers Internet access as a civil right, fundamental to the exercise of citizenship, freedom of expression and access to information. Therefore, it focuses on the guarantee of rights, considering the technical and social particularities of information in the digital environment.

It is a law that could create a safeguard for websites as it prevents the removal of Internet contents without a judicial order. The proposal also foresees the introduction of limits on the storage and use of personal data. Both aspects are seen as pillars of the protection of privacy and freedom of expression. This law may be regarded as highly innovative and inspiring due to the way in which the process has been conducted and the issues being discussed.

This paper shows the key aspects of the Brazilian project, how controversial issues are managed and highlights their innovations and limitations.

2. Current Situation in Brazil

Freedom of expression and Privacy

In recent years, there have been a number of initiatives related to censorship in Brazil several. In

January, 2010, the Court of Justice in São Paulo ordered You Tube access to be cut for all Brazilian users following demands made by of a famous model unhappy about a video made by a "paparazzi" (UOL Tecnologia, 2007). This measure was the cause of intense discussion in the media. The order was cancelled two days later after massive criticism from internet users.

According to the NGO Article 19, more processes are brought against journalists in Brazil than any other country with 3,133 processes against 3,237 journalists (ConJur, 2007a; 2007b).

There are no reliable statistics on censorship, but there are numerous cases of juridical pressure on bloggers resulting in a climate of fear in the so called blogsphere. In Brazil, this is such a frequent problem that the cyberactivists refer to it as "blog bullying". Most cases involve the expression of negative opinions or complaints about companies, services or politicians (WikiPP, 2010).

There is also no reliable data on privacy, but the following example demonstrates the current situation: between July 1st, 2009 and December 31st, 2009, the Brazilian authorities made 3,663 requests for the removal of data from Google and You Tube. Brazilian is in first place in Google's World Ranking (Google, 2010), followed by USA (3,580) and UK (1,166,). Brazil again holds the first place for removal request with 291 demands, followed by Germany with 188 requests.

Copyright violation

A study conducted in 2009 by Barbosa and Craveiro (2010) indicated that there were 298,181 complaints of incidents of security risk to the Internet Management Committee of Brazil (CGI in Portuguese between January and June in 2009,. Of these, 233,604 cases were referred as "fraud". Analysing the details of the "fraud" caption, the study shows that about 217,000 records are related to copyright infringement. It is noteworthy that the academic literature does not consider breach of copyright by in the area of Information Security as a kind of security attack on systems[4].

Copyright infringement was responsible for 96.06% of all fraud in the first half of 2009. The complaints were made by the Associação Antipirataria de Cinema e Música (APCM) — Antipiracy Association of Music and Movie —, an entity linked to MPA (Motion Picture Association) and the IFPI (International Federation of the Phonographic Industry).

Through pressure from their lawyers, the APCM has also removed thousands of pages and links to

4 The academic literature divides the attacks on the security of systems in fields of type: Authentication deals with identity of users or data source; Access Control limits and controls access to the system and applications connected by a means of data transfer; Confidentiality of data, both on account of the connection, the selected field or flow of traffic; Data Integrity which ensures that data received are the same as those of the sender; Nonrepudiation allowing non-denial by both the source and destination; Service Availability which ensures that a system or application will be accessible and usable when requested. (STALLINGS, 2007, ac. Craveiro, 2010):

websites and blogs. The fear of facing lawsuits has resulted in the decline of Internet users, even when the removed content does not have license problems. APCM announced the withdrawal of 118,750 links of movies and music, the removal of 22,113 posts in blogs and 20,332 links to P2P files (APCM, 2010) in the first halfof 2009, Under pressure from APCM, entire blogs have also been removed .

Although this has impacted the Media, the result is unsatisfactory because the links can be replaced and easily found on P2P networks through search engines. There is also widespread use of file-hosting sites like Rapid Share or Mega Upload.

Frauds and Paedophilia

The combat of frauds and paedophilia is the main argument used **openly** in Brazil to defend the storage of logs of internet providers or services providers.

The most active pro-monitoring lobby comes from the Brazilian Federation of Banks, which claims millions of losses with fraud. However, the banks do not use secure systems like cryptographics keys. This could cost much more than lobbying in favour of proposal a law that determines control over the Internet[5] . On the other hand, there is discussion on whether the Law permits the use of cryptograpgic key because the Constitution guarantees freedom of expression, but does not allow anonymity.

As for paedophilia there is an active NGO called SaferNet in Brazil that harasses politicians and governmental authorities to improve the monitoring of internet users and implement more restrictive policies on the digital environment. SaferNet has promoted a public audience with the Attorney General of "Ministério Público**"** (literally *Public Ministry*) (MPF, 2010; Machado, 2009) to convince judges and authorities of the the importance of enforcing data retention policy of logs. It is interesting to note that the paedophilia lobby has been working together with the banking lobby to improve controls on the internet.

Therefore, the current status of the law enforcement in Brazil is characterized by uncertainty. In the Brazilian Civil Code, reformed in 2003, there is no reference to the Internet. In this scenario, judges lack knowledge and technical references and therefore have to make decisions based on very subjective interpretations of outdated laws.

---

5 The bank sector gave strong support to the Law Proposal 76/2000 known as "Azeredo Proposal" (CPD, 2006), because it was proposed by Senator Eduardo Azeredo, a right-wing politician linked with the financial sector. This proposal has generated several protests from civil society. In March, 2009, the federal government – with majority in the Congress and Senate- was pressured to make the political decision to block the proposal. It was probably one of the main reasons for the proposal of the Civil Rights Framework for Internet.

3. Key issues in the Brazilian government proposal

Although the proposed Bill aims to achieve a harmonious relationship between connection providers, service providers, different types of user and public authority, it is deeply focused on civil rights.

The 2nd article stipulates that the regulation of Internet in Brazil "shall be grounded on the recognition of the international nature of the Internet; the rights of citizenship into the digital environment; the human rights; the values of plurality, diversity, openness, and collaboration; the freedom of entrepreneurship and the freedom of competition", listing the following principles:

> I - the guaranteed freedom of speech, communication and expression of thought;
> II - protection of privacy;
> III - protection of personal data in accordance with the law;
> IV - preservation and guarantee of net neutrality;
> V - preservation of stability, security and functionality of the network, ensuring means of technical measures compatible with international standards and incentives for best practices;
> VI - preservation of the participatory nature of the Internet.

The bill has other strengths, establishing:

- the fostering of standardization, accessibility and interoperability through the use of open standards.
- quality of internet connection;
- preferential adoption of open technologies, standards and formats;
- (for governmental websites) strengthening participatory democracy; transparent, collaborative, and democratic mechanisms of governance with participation of the various sectors of society; promoting interoperability of technology for e-government services;
- disclosing and disseminating data and public information in an open and structured manner;
- optimization of network infrastructure, promoting technical quality, innovation, and the dissemination of Internet services, without impairing the openness, neutrality and participatory nature of the Internet.

Despite the well written text and the modern approach, the law has extremely controversial points such as whether or not connection logs can be stored, what type of data can be stored, time storage of such records, removal mechanisms of site content — as well as for the third parties —, and the role of connection providers and service providers.

These discussions are directly affected by the different interpretations of the scope and limits of freedom of expression, as well as the political positions on the balance between access to information and property rights in the digital environment. This scenario puts in different sides of cultural industry, agencies collectors copyright, security agencies, organizations and civil rights, consumer rights, internet users and divides scholars and experts. Below we summarize the main points of the proposal:

Table 1 — Points of the Proposal — Brazilian Bill of "Civil Rights Framework for Internet" — 2010

Storage or not of connection logs	Yes
Time storage of such records	Maximum term 6 months. There is not a minimum time. Aplicable just to ICP logs. There is not need to keep ISP logs.
Liability	The obligation to maintain records on connection logs cannot be transferred.
Type of data that can be storage by Internet Connection Providers (ICP)	Only on connection logs. Its forbidden to keep records on Internet services access logs.
Desclosure of conection logs by ICP	only by a court order or by prior written permission of the respective users
Type of data can be storage by Internet Service Providers (ISP)	The maintenance of Internet services logs **shall depend on the express authorization** of the user about the nature, finality, period of keeping, safety policies and destination of the information recorded, allowing the user to access, correct and update the information when requested. Idem about the management, disclosure to third parties or the publication of the information recorded;
Desclosure of user's record datas	Only by a court order.
Crossing data connection logs and services	The crossing of Internet services logs and access logs can only be disclosed by means of a court order.
Liability of ISP under contents	The ISP may only be liable for damages arising out of content generated by third parties if the provider receives a court order, and fail to comply with its ruling.
Liability of ICP under contents	The ICP are not liable for damages resulting from content generated by third parties. **(It is prevents any "three strikes" approach)**
Legal Procedures to removal contents	The court notification shall contain, under penalty of invalidation: a) identification of the applicant, including full name, civil registry and fiscal identification numbers and current contact information; b) date and time of transmission; c) clear and specific identification of the content signalled as harmful to enable unambiguous locality of the notified material; d) description of the relationship between the applicant and the content identified as harmful; and e) legal justification for removal.
Procedures to judicial requests for logs	The judge must dispatch a warrant requesting the party responsible for maintaining the records to provide Internet services access logs or connection logs. The application shall include the detailed description of evidence concerning the occurrence of an illegal act; the indispensable need of the requested logs for investigating the illegal act; the period to which the records are related to.

	The request for providing Internet services access logs will be subjected to the proof that the responsible party maintains such records with the express authorization of users. If the provision of ISP access logs are not needed for investigation, the judge shall limit the request only to connection logs. The judge is responsible for ensure the secrecy of communications and to preserve the intimacy, privacy, honour, and user image, being able to determine whether the information should be kept under secrecy in court records.
Network Neutrality	The responsible for transmitting, switching or routing has the obligation of treating equally every data packages, content, terminal or application, being forbidden of any discrimination or degradation of traffic not related to technical requirements aiming at preserving the quality of service contracted.
On protecting privacy of Internet Communications	The procedures for intercepting, wire-tapping, or infringing the content of Internet communications may only occur for purposes of criminal prosecution and will be ruled by the law that deals with the interception of telephone communication and telematic data.

4. Responses and proposed amendments to the draft text: conflicting interests

The bill received countless contributions and criticisms. Below we analyze the most important, concentrating our analysis on the key points and role played by leading actors.

Many entities that are engaged in intellectual property protection and therefore interested in more regulation and controls on the Internet sent their proposals e.g. IIPA(International Intellectual Property Alliance), IFPI (International Federation of the Phonographic Industry), ABPD (Brazilian Association of Discs Producers), MPAA[6] (Movie Picture Association American), Entertainment Software Association (USA), FILAIE (Iberian-Latin American Federation of Performers), AMPROFON (Mexican Association of Phonogram and Videogram), CAPIF (Argentine Chamber of Phonograms and Videograms Producers), Society of Authors and Composers of Mexico (SACM), Brazilian Movie Union (UBV) as well as a number of Law Offices. Brazil is one of the most important markets of the music, movies, software and entertainment industry in general.

MPAA call for the creation of "a regime of vicarious liability that encourages Internet providers to cooperate with right holders in combating illegal activities online". MPAA wants this to be done by "[using] network management tools, including recognition technology content"; using "precautionary measures and injunctions" against violations of intellectual property rights, and allowing information to be obtained about the records of access to Internet services without the express authorization of users through the courts including injunctions, (MPAA, 2010).

6 The contribution of MPAA was signed by "MPA Brasil", a local representative of the organization.

IIPA has a more forceful perspective on the legal restrictions that should be imposed on Internet users. IIPA is comprised of seven member associations: the Association of American Publishers (AAP), the Business Software Alliance (BSA), the Entertainment Software Association (ESA), the Independent Film & Television Alliance (IFTA), the Motion Picture Association of America (MPAA), the National Music Publishers' Association (NMPA) and the Recording Industry Association of America (RIAA). According to IIPA, the seven member associations represent over 1900 U.S. companies producing and distributing materials protected by copyright laws throughout the world. It includes all types of computer software, including business applications software and entertainment software (such as videogame discs and cartridges, personal computer CD-ROMs, and multimedia products); theatrical films, television programs, DVDs and home video and digital representations of audiovisual works; music, records, CDs, and audiocassettes; and textbooks, trade books, reference and professional publications and journals. (IIPA, 2010).

IIPA made strong and direct criticisms of the proposed Bill. Aligned with their efforts to "improve international protection of copyrighted", IIPA claims that "elements of the bill would remove incentives for cooperation between right holders and Internet Service Providers, and could stifle development of effective tools and policies for combating online infringement (...) and pre-empt the potential use of a variety of mechanisms to address online piracy." (IIPA, 2010b).

But the most detailed criticisms of the copyright industries came from International Intellectual Property Alliance. IFPA represents the recording industry worldwide with a membership of some 1400 record companies in 66 countries and affiliated industry associations in 45 countries. IFPA 's mission is "to promote the value of recorded music, safeguard the rights of record producers and expand the commercial uses of recorded music in all markets where its members operate." (IFPA, 2010a).

The contribution of IFPA to the proposed Bill (2010b) has three key points: i) The importance of copyrights in the online environment; ii). A "net neutrality" that allows the ISP to discriminate between legal and illegal content and services; iii) the need for "incentives" for Internet Service Providers to take action to address online piracy.

According to IFPA 's proposal "assuming that the goal of neutrality is pursued, it should not be read to eliminate the vital distinction between lawful content and illicit material (...) It could also frustrate potential voluntary efforts by ISPs to stem the flow of illegal traffic going over their networks. (...) The overbroad definition set out in the Draft Proposal would therefore constitute a drastic step with a major negative impact not only on ISPs, but also on all copyright industries (...). Any regulation on net neutrality must be done with care, in order not to inadvertently protect the

dissemination of illegal content."

The IFPA document calls the ISPs "gatekeepers of the Internet". "They [ISPs] should be appropriately incentivised to cooperate with rightholders in the fight against online infringement."

According to IFPA "many countries have adapted their laws accordingly, ensuring legal incentives for ISPs to take reasonable and effective action against various forms of piracy." But the IFPA proposal did not indicate any country or regulatory system that works in this way.

The IFPA argues that "more and more countries are considering new solutions to address online piracy that involves content that is not hosted on ISP servers but resides on individual users' computers and is distributed over peer-to-peer file-sharing networks"; it recommends, actually, the application of "*graduated response* mechanisms with deterrents, sanctions available against repeat infringers who ignore a series of notices and warnings".

The IIPA's proposal concludes with an ironic criticism of those who drafted the bill by suggesting its improvement by intellectual property experts:

> The approach of the Draft Proposal should therefore be rethought and amended substantially with the input of IP experts and the direct involvement of the copyright and cultural communities to establish an appropriate legal framework providing the necessary conditions for legitimate markets to develop online. The central prerequisite is the recognition of the need for effective protection of copyright and the ability to ensure that action can be taken against, unlawful conduct.

It should be noted that IIPA collected the most information for The Special 301 Report, prepared by the Office of the United States Trade Representative, where Brazil is listed on the "watch list". According to section 301 of the Trade Act of 1974, U.S. may impose sanctions on countries that violate trade rights. Internationally, IIPA puts the most pressure on Brazil to stiffen the IP laws.

Apart from private individuals, organizations from civil society and consumer rights organizations sent their contributions, e.g. IDEC, PRO TESTE. In general, the contributions from civil society strengthen the proposal subject to consultation by the Ministry of Justice. The only item that received very severe criticism was the requirement for providers to store logs. The majority of civil society organizations advocated non mandatory of storage of logs.

The Federal Police sent their contribution calling for a significant increase in restrictions, such as increasing the data storage of connection logs for a minimum of three years, access to data without court order and prohibiting the use of cryptographic keys, among other measures.

As for the Draft proposal on the time of data log storage, the Federal Police are very ironic: "staying

with this time, would be cause for celebration for organized crime would find incentive to use the Internet to practice their illegal actions" (Polícia Federal, 2010). The Federal Police responds to the civil rights organizations by also defending the access to users' data by "police authority", without the need of a court order. The Federal Police is an institution which comes under the Ministry of Justice and the lobby for "security" therefore has an important ally inside the Ministry.

5. Conclusion: control or freedom?

Control or freedom? The wide range of actors took a public position. In some ways, the "Civil Rights Framework for Internet" serves as a kind of a microcosm of the movement that is found worldwide in the dispute on the regulation of the Internet. In addition, it is increasingly clear that entities want to control or ensure that civil liberties are aligned to them side, strengthening their positions.

Everything indicates that whatever the decision must be predominantly a political one. Which side do we take: the right to property, security and control or freedom of access to culture and information? Ironically, digital technologies have great potential for sharing and monitoring.

Do we defend the "old intellectual property", of "security and control" or the freedom of access to information and culture? We must therefore face a challenge. In the words of Yoshai Benkler in his book *The Wealth of Networks*:

> There is no guarantee that networked information technology will lead to the improvements in innovation, freedom, and justice that I suggest are possible. That is a choice we face as a society. (Benkler 2007:18)

If the Proposed Bill of Civil Rights Framework for Internet remains unchanged, it will be a very liberal choice. Let's see the reaction from lobbies when sent to parliament.

6. References

APCM (2010) *APCM divulga estatísticas de pirataria na internet*. Available on Internet http://www.apcm.org.br/conteudo_geral.php?ID_NOT=107&TARGET=HST

Barbosa, David P.; Craveiro, Gisele S (2010) *Estudo Técnico da Legislação nº 89 de 2003 acerca da Internet Brasileira*. Cadernos GPOPAI, n 5.

Benkler, Y. (2007) *The Wealth of Networks*. Yale University Press. New Haven, Conn: Yale University Press. Available on Internet http://cyber.law.harvard.edu/wealth_of_networks/Main_Page.

Brazilian Ministry of Justice (2010) *Civil Rights Framework for the Internet in Brazil. Bill Proposition for Collaborative Debate*. Available on Internet https://docs.google.com/fileview?id=0B-a4T5El0jxuZDcxMDMzNmItZTc5Ny00MmU4LTllMTktNTUyMThiOGI5MmYw&hl=pt_BR

ConJur – Consultor Jurídico. (2007a) *Brasil bate recorde mundial em ações contra jornalistas*. Available on Internet http://www.conjur.com.br/2007-out-05/brasil_bate_recorde_mundial_acoes_jornalistas

_____ (2007b) *Valor médio de indenizações contra imprensa sobe para R$ 80 mil*. Available on Internet http://www.conjur.com.br/2007-mai-31/aumenta_valor_medio_indenizacoes_imprensa

CPD (2006) PLS - PROJETO DE LEI DO SENADO, Nº 76 de 2000. Available on Internet http://www.cpd.furg.br/bin/noticias/index.php?id_noticia=13

Google (2010) *Government requests directed to Google and YouTube*. Available on Internet http://www.google.com/governmentrequests/

IFPI (2010a), IFPI's Mission. http://www.ifpi.org/content/section_about/index.html

___ (2010b) IFPI submission on the Draft Proposal for a Regulatory Framework for the Internet. http://culturadigital.br/marcocivil/2010/05/26/contribuicao-do-ifpi-para-o-marco-civil-da-internet/

IIPA, 2010. Description of IIPA. http://www.iipa.com/aboutiipa.html or http://www.iipa.com/pdf/IIPAFactSheet091609.pdf

____ (2010b) C*omments on the Draft Bill Proposition on a Civil Rights Framework for the Internet in Brazil ("Internet Bill")* . Available on Internet http://culturadigital.br/marcocivil/2010/05/26/contribuicao-do-iipa-para-o-marco-civil-da-internet/

Machado, Jorge (2009) *Relato da audiência pública no MPF sobre armazenamento de logs*. Available on Internet http://www.gpopai.usp.br/wiki/index.php/Relato_da_audi%C3%AAncia_p%C3%BAblica_no_MPF_sobre_armazenamento_de_logs

Marco Civil (2010) *Comments on Draft Bill Proposition on Civil Rights Framework for Internet in Brazil*. Available on Internet http://culturadigital.br/marcocivil/2010/04/20/draft-bill-propostion-on-civil-rights-framework-for-internet-in-brazil/

MPAA (2010) *Consulta Pública do Anteprojeto de Lei sobre o Marco Civil da Internet*. Available on Internet http://culturadigital.br/marcocivil/2010/05/29/contribuicao-da-mpa-brasil/#more-1757

MPF (2010) *Notícias do MPF*. Available on Internet http://www.gpopai.usp.br/wiki/index.php/Chamada_para_audi%C3%AAncia_do_MPF_sobre_armazenamento_de_logs (mirror) http://www.pgr.mpf.gov.br/noticias/noticias-do-site/consumidor-e-ordem-economica/audiencia-publica-no-mpf-sp-debate-armazenamento-de-logs-de-acesso-a-internet/ (site not avaliable) (Cache Google http://webcache.googleusercontent.com/search?q=cache:EWCeQade6coJ:www.pgr.mpf.gov.br/noticias/noticias-do-site/consumidor-e-ordem-economica/audiencia-publica-no-mpf-sp-debate-armazenamento-de-logs-de-acesso-a-internet/+armazenamento+de+logs+audiencia+p%C3%BAblica&cd=1&hl=pt-BR&ct=clnk&client=firefox-a)

Polícia Federal (2010) *Contribuição da Polícia Federal para o Marco Civil da Internet*. Available on Internet http://culturadigital.br/marcocivil/2010/05/31/contribuicao-da-policia-federal-para-o-marco-civil-da-internet/#more-1839

STALLINGS, W. (2007) *Criptografia e Segurança de Redes: Princípios e Práticas*. 4th edition. Pearson/Prentice Hall, São Paulo.

UOL Tecnologia (2007). *Entenda o processo que levou ao bloqueio do YouTube*. Available on Internet http://tecnologia.uol.com.br/ultnot/2007/01/09/ult4213u7.jhtm

Wiki PP (2010) *Blog_Bullying*. Available on Internet http://partidopirata.org/wiki/index.php/Blog_Bullying

7. Appendix

NEW DRAFT BILL PROPOSITION FOR COLLABORATIVE DEBATE

Sets forth the Civil Rights Framework for the Internet in Brazil.

THE NATIONAL CONGRESS decrees:

CHAPTER I

PRELIMINARY PROVISIONS

Article 1. This law sets forth rights and obligations concerning the use of the Internet in Brazil, and provides guidelines over the matter for the jurisdictions of Federal Union, States, Cities and the Federal District of Brasilia.

Article 2. The regulation of Internet in Brazil shall be grounded on the recognition of the international nature of the Internet; the rights of citizenship into the digital environment; the human rights; the values of plurality, diversity, openness, and collaboration; the freedom of entrepreneurship and the freedom of competition, considering the following principles:

I - the guaranteed freedom of speech, communication and expression of thought;

II - protection of privacy;

III - protection of personal data in accordance to the law;

IV - preservation and guarantee of net neutrality;

V - preservation of stability, security and functionality of the network, ensuring means of technical measures compatible with international standards and incentives to best practices;

VI - preservation of the participatory nature of the Internet.

Sole Paragraph. The principles defined by this law do not exclude others set forth by national legal system related to the matter, or by the international treaties signed by the Federative Republic of Brazil.

Article 3. The regulation of the use of the Internet in Brazil will have the following objectives:

I – to guarantee Internet access to all citizens;

II – to promote access to information, knowledge and participation in cultural activities;

III - to strengthen free enterprise and free competition;

IV - to promote innovation and to foster the wide dissemination of new technologies and models of use and access, and

V - to promote standardization, accessibility and interoperability through the use of open standards.

Article 4. For effects of this Law, the follow definitions shall be applied:

I - Internet: the set of means of transmission, switching and routing of data, structured internationally, as well as the protocols necessary for communication between terminals, including also the software required to this specific end;

II - terminal: a computer or similar device that connects to the Internet;

III - administrator of autonomous system: the legal entity duly registered by the Latin American and Caribbean Internet Addresses Registry (LACNIC), responsible for specific set of IP *(Internet protocol)* numbers and by a set of routers, networks and Internet communication lines, which are part of an infrastructure defined by the same protocols and metrics.

IV - Internet connection: authentication of a terminal for sending and receiving data packages though the Internet, by means of the attribution of an IP number;

V - connection logs: the set information referring to the date, time of beginning and ending of an Internet connection, its duration and the IP number used by the terminal for receiving data packages;

VI - Internet services: the set of diverse services that can be accessed through a terminal connected to the Internet, such as, but not limited to, navigation, instant messaging, sending and receiving e-mails, publishing of texts or audiovisual works in digital formats, among others;

VII - Internet service access logs: the set of information referring to the date and time of use of a particular Internet service by a determined IP number.

Article 5. This Law shall be construed taking into account not only the principles, objectives and directives established herein, but also the nature of the Internet, it´s particular uses and customs, it´s importance regarding the promotion of human, economic, social, and cultural development, the requirements for promoting the public good, and the rights and obligations applicable to individuals or groups.

CHAPTER II

ON THE RIGHTS AND OBLIGATIONS OF USERS

Article 6. The access to Internet is a civil right, essential for the exercise of citizenship, of the freedoms of

expression, speech and thought, and to guarantee the access to information.
Article 7. The Internet user has the right:
I - to inviolability and privacy of its communications, except in case of a court order, under the specific clauses determined by law, for the purpose of criminal investigation or under a criminal process;
II - to the non-suspension and non-degradation of the contracted quality of the Internet connection, as provided by Article 12, except in the case of default of payment, directly related to the utilization of the service;
III - to get clear and comprehensive information written in the contracts with providers, expressing the regime of protection of personal data, connection logs and Internet service access logs, as well as information on the practices of network management adopted that might affect the quality of service offered, and
IV - to the non-disclosure or use of it´s connection logs and Internet services access logs, except under express consent or due to a court order.
Article 8. The full exercise of the right to Internet access has as requisite the guarantee to the right of privacy and freedom of expression in communications.
Sole Paragraph. Internet users are allowed to adopt safety measures for safeguarding the protection of personal data and secrecy of communications, in the exercise of the rights of privacy and freedom of expression.

CHAPTER III
ON THE PROVISION OF INTERNET CONNECTION AND SERVICES
Section I
General Provisions

Article 9. The Internet connection provision imposes the obligation of keeping records only on connection logs, under the terms of Subsection I and Section III of this chapter. The connection providers are forbidden to keep records on Internet services access logs.
Sole Paragraph. The Internet connection providers shall not monitor, filter, analyze or inspect the content of data packages, except for the technical administration of traffic, under the provisions of Article 12.
Article 10. Providing Internet services, whether onerous or free of charge, does not oblige the service provider to monitor, filter, analyze or monitor the contents of data packages or to keep records of Internet services access logs, except in cases of specific court order, subjected to the provisions of Article 18.
Sole Paragraph. For the effects of this provision, users who hold powers of moderation of content produced by third parties shall be considered under the same obligations as the Internet services providers.
Article 11. The liability of the Internet services providers for damages arising from content generated by third parties is conditioned to the violation of the procedures set forth by Section IV of this chapter.

Section II

On data traffic
Article 12. The responsible for transmitting, switching or routing has the obligation of treating equally every data packages, content, terminal or application, being forbidden of any discrimination or degradation of traffic not related to technical requirements aiming at preserving the quality of service contracted.

Section III
On data records
Subsection I

The custody of connection logs
Article 13. The maintenance and disclosure of records on connection logs regulated by this law must abide to the preservation of privacy, intimate life, reputation, and image of the parties directly or indirectly involved.
Article 14. The provision of Internet connection imposes to the administrator of an autonomous system the obligation to keep records on connection logs confidentially, in a secured controlled environment, for the maximum term of 6 (six) months, as provided by further administrative regulation.
Sole Paragraph. The obligation to maintain records on connection logs cannot be transferred.
Article 15. In maintaining connection logs records:
I - the connection logs can only be disclosed to third parties by means of a court order or by prior written permission of the respective users;
II - user personal data can only be disclosed and linked with the connection logs by means of a court order;
III - the management, safety and confidentiality procedures and practices related to maintaining connection logs records and user personal data must be clearly informed to the users.
Sole Paragraph. The security procedures necessary for preserving the confidentiality and integrity of the connection logs and of the users personal data referred in this article must follow adequate standards, to be

defined by further regulation.

Subsection II

On custody of Internet services access logs

Article 16. The maintenance of Internet services access logs shall depend on the express authorization of the user and shall be bound to the following provisions, without prejudice of other norms and directives related to the protection of personal data:

I - prior information to the user about the nature, finality, period of keeping, safety policies and destination of the information recorded, allowing the user to access, correct and update the information when requested;

II - prior informed consent and awareness of the user about the management, disclosure to third parties or the publication of the information recorded;

III - data that allow identification of the user can only be disclosed and linked to the Internet services access logs by means of a court order.

Article 17. Damages caused to owners of personal information must be repaid on terms of law.

Subsection III

On protecting privacy of Internet Communications

Section 18. The procedures for intercepting, wiretapping, or infringing the content of Internet communications may only occur for purposes of criminal prosecution and will be ruled by the law that deals with the interception of telephone communication and telematic data.

Section IV

On the content removal

Article 19. The Internet connection provider will not be liable for damages resulting from content generated by third parties.

Article 20. The Internet service provider may only be liable for damages arising out of content generated by third parties if the provider receives a court order, and fail to comply with its ruling, in order to take the measures within its scope of service and within the defined term to make the content the court signaled as infringing unavailable.

Article 21. The court order described on Article 20 shall contain, under penalty of invalidation:

I - identification of the applicant, including full name, civil registry and fiscal identification numbers and current contact information;

II - clear and specific identification of the content signaled as harmful to enable unambiguous locality of the notified material;

III - description of the relationship between the applicant and the content identified as harmful; and

IV - legal justification for removal.

Article 22. After removing the content, Internet service providers will be responsible to report this action to the user who has produced the content, quoting the reasons for the court order, whenever the user responsible for the infringing content is identifiable.

Article 23. Users who possess administrative powers to manage content will be treated alike Internet service providers for the purposes of the clauses described in this Section. (preserved)

Article 24. Both the party that reports harmful content and the party that contests the removal of the content will be held responsible for any false or erroneous information they provide, as well as for abusive behavior or bad faith, in accordance to the law. (suppressed)

Article 25. Users who possess administrative powers to manage content will be treated alike Internet service providers for the purposes of the clauses described in this Section. (suppressed)

Section V

On judicial requests for logs

Article 26. The interested party may, for the sole purpose of gathering evidence in legal proceedings, request a judge to dispatch a warrant requesting the party responsible for maintaining the records to provide Internet services access logs or connection logs.

Sole Paragraph. In the application for a judicial warrant the party shall include:

I - the detailed description of evidence concerning the occurrence of an illegal act;

II - the indispensable need of the requested logs for investigating the illegal act, and;

III - the period to which the records are related to.

Article 27. The judicial warrant for providing records will follow the applicable procedural rites, in observance of the following:

§ 1. The request for providing Internet services access logs will be subjected to the proof that the responsible party maintains such records with the express authorization of users, also in compliance with the provisions of Article 16.

§ 2. If the provision of Internet services access logs are not needed for investigation, the judge shall limit the request only to connection logs.
§ 3 The judge is responsible for taking the necessary steps to ensure the secrecy of communications and to preserve the intimacy, privacy, honor, and user image, being able to determine whether the information should be kept under secrecy in court records.

CHAPTER IV
ON THE ROLE OF PUBLIC AUTHORITIES

Article 28. The Federal Union, States, Cities and Federal District of Brasilia shall abide for the following principles for the development of the Internet in Brazil:
I - establishment of transparent, collaborative, and democratic mechanisms of governance with participation of the various sectors of society;
II - promoting interoperability of technology for e-government services in different levels of the Federation, to allow the exchange of information and streamline of procedures;
III - promoting interoperability between different systems and terminals, especially among different levels of the federation and several sectors of society;
IV - preferential adoption of open technologies, standards and formats;
V - disclosing and disseminating data and public information in an opened and structured manner;
VI - optimizing network infrastructure, promoting technical quality, innovation, and the dissemination of Internet services, without impairing the openness, neutrality and participatory nature of the Internet;
VII - developing initiatives and Internet-use-education programs;
VIII - promoting culture and citizenship, notably by providing more dynamic and efficient public services;
IX - efficient use of public resources and digital services available to citizens, and
X - providing citizen-care public services in a integrated, simplified fashion through multiple communication channels.
Article 29. Government sites and portals should strive for:
I - compatibility of e-government services with the various terminals, operating systems and applications used to access them;
II - accessibility for all interested parties, irrespective of their physical, motor, perceptual, cultural, and social skills, provided that confidentiality issues and legal and administrative regulations are respected;
III - compatibility with both human reading and machine treatment;
IV - easy understanding of electronic government services, and
V - strengthening participatory democracy.
Article 30.
Providing training for using Internet as a tool of citizenship and for promoting culture and technological development are part of the compliance with the constitutional duty of the State to promote education at all levels.
§ 1 Without prejudice to the powers of government, the State will encourage private initiatives that promote the Internet as an educational tool.
§ 2 Internet training should be integrated with other educational practices.
Article 31. Public initiatives to promote digital literacy and the usage of Internet as a social tool must:
I - seek to minimize inequality of access to information, especially between regions;
II - promote digital inclusion of all population, especially low-income individuals.
Article 32. The State must seek, formulate and promote regular research and periodically set objectives, strategies, plans and time lines regarding the use and development of the Internet in the country.

CHAPTER V
FINAL PROVISIONS

Article 33. The Internet users´ interests and rights shall be exercised either individually or collectively, regarding provisions of Articles 81 and 82 of Law 8078 of September 11, 1990.
Article 34. This Law shall enter into force upon its publication.