## "Cyber Censorship in India and China"

Yogesh Vishnoi KIIT Law School, Bhubaneshwar Siddhant Mishra KIIT Law School, Bhubaneshwar

#### **Abstract**

Everyone has an opinion, and the guy screaming for censorship may be next guy to have his ideas cut off.

This paper looks at cyber censorship and aims at using this example as a means to generalize laws as a whole. Different aspects of the law have been discussed with the countries of India and China in mind. These two countries have been picked keeping in mind the vastly different systems of government. Comparison of different aspects of the law between these countries, and posing intriguing questions that aim at addressing legitimacy of laws are two of the highlights of the project. Cyber censorship means control or suppression publishing of, or access to information on the internet .Mainly it done by Governments or by the private organizations at the behest of government or by the regulators Internet censorship affects everyone. China is arguably one of the most restrictive countries in the world. The Government in China has passed numerous regulations to control, among other things, online sources of information and free debate.

The aim of the paper is to provide a detailed and critical study of laws pertaining to cyber censorship in India and China, issues which have been the focus of many a debate. The researchers have examined case law and writings and prepared a critique of the said topic.

Key-Words: Cyber, Censorship, Harmful Information, Democracy, Regulation.

<sup>\*</sup> YOGESH VISHNOI, 9<sup>th</sup> semester, (IPR HONS.) KIIT Law School, Bhubaneswar-751024, yogeshvishnoi.kls@gmail.comMob: - +917381337267,

<sup>\*</sup>Siddhant Mishra, 9<sup>th</sup>semester, (CRIMINAL HONS.) KIIT Law School, Bhubaneswar-751024, <u>siddhantmishrakls@gmail.com</u>

#### Introduction

This project looks at cyber censorship and aims at using this example as a means to generalize laws as a whole. Different aspects of the law have been discussed with the countries of India and China in mind. These two countries have been picked keeping in mind the vastly different systems of government. Comparison of different aspects of the law between these countries, and posing intriguing questions that aim at addressing legitimacy of laws are two of the highlights of the project.

## **Research Methodology**

The researchers have adopted the doctrinal form of research in preparing this project. As the project is an analysis laws pertaining to cyber censorship in India and China, this form of research was most appropriate. The research is primarily based on books, articles, case law, and acts.

#### **Research Scheme**

## 1.2.1 Aims and Objectives

The aim of the paper is to provide a detailed and critical study of laws pertaining to cyber censorship in India and China, issues which have been the focus of many a debate. The researchers have examined case law and writings and prepared a critique of the said topic.

## 1.2.2 Scope and Limitations

Within the scope of this paper, the researcher presents the legal provisions pertaining to cyber censorship, the gap between passing of a Bill and its implementation, a comparison of various aspects of the laws governing cyber censorship between India and China, and a critical view at legitimacy of laws.

## 1.2.3 Chapterization

The paper is divided into three chapters. First, it begins with a discussion of the different forms of government, the provisions of law related to cyber censorship, and the issues stemming from it. The second chapter looks at the reactions to these laws, the consequent action that the government has to take, and the positive and negative aspects of these laws; and the third examines critically the legitimacy of the laws.

## **Systems of Governance**

This chapter discusses the two systems of governance that exist in the two countries which are the focus of this project: authoritarian democraticand how these systems of governance significantly influence the manner in which are enacted and implemented in the two previously mentioned countries.

## 1.1.SEPARATION OF POWERS- THE INDIAN PLAN

The 'Doctrine of Separation of Powers', is an integral part of the Indian Constitution despite there being no express provision recognising it as such. A reasonable demarcation of powers among the three organs of the Government, viz. legislature, executive and judiciary- is implicitly provided for through a number of Articles.

For example, Article 53(1), vests the executive power of the Union in the President, while Article 154 vests the executive power of the State in the Governor. Judicial power is to be exercised by a hierarchy of courts, with the Supreme Court at the apex. Further Article 50 provides for a complete separation of the judiciary from the executive.

The 'Doctrine of Separation of Powers' in India has also evolved through a series of judgments. The Supreme Court, in the case of *BandhuaMuktiMorjhav*. *Union of India*, stated that although the division is not precisely demarcated, there is a general acknowledgment of its limits within certain measure of overlapping.<sup>1</sup>

While this doctrine is widely accepted, in practice however, due to the ambiguous manner in which it has been addressed in the Constitution there have been disputes from time to time regarding the scope and ambit of each organ. For example, in *KesavanandaBharativ*. *State of Kerala*, the Supreme Court looked at the power of the legislature to amend the Constitution. It affirmed that the 'basic structure' of the Constitution could not be amended, even by an Act of the Parliament.<sup>2</sup>

## 1.2.SEPARATION OF POWERS IN CHINA

The Constitution of China also envisages a system of separation of powers wherein it provides for a legislature, executive and judiciary, each with its own functions which are to be exercised independently of each other. The National People's Congress and its Standing Committee exercise the legislative power of the State whereas the State Council or the Central People's Government is the executive body of State administration as per Articles 58 and 85 respectively. Judicial function is exercised by the Supreme Court and local people's courts. This has been given in Article 124. Also Article 129 provides for the establishment of People's Procuratorates which are State organs for legal supervision.

<sup>&</sup>lt;sup>1</sup> AIR 1984 SC 80

<sup>&</sup>lt;sup>2</sup> AIR 1973 SC 1461

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

The supreme sovereign power is in the hands of the NPC- interpreting and amending the Constitution, making laws, and selecting Government officers.<sup>3</sup> This has almost rendered the separation of powers to be nonexistent.

Theelection process is an extremely constrained one with opposition or unorthodox candidates almost never winning. <sup>4</sup> Thus much of the legislative and executive power is wielded by the Communist Party.

## 1.3.CYBER CENSORSHIP LAWS AND POLICIES

Following are the censorship laws and policies of the country:

## 1.3.1. INDIA

Internet censorship in India is mainly governed by the IT Acts. It began around the end of the Kargil war, when the government tried to block access to a Pakistani newspaper "Dawn" by denying access to it by VSNL, which had a monopoly to Internet services at the time. Subsequently, the Information Technology Act was passes in 2000, and the Information Technology (Amendment) Act in 2008. In 2011, the Government also passed the Information Technology Rules.

## 1.3.1.1.INFORMATION TECHNOLOGY ACT 2000

The Information Technology Act 2000 was the first cyber law to be passed in India. It was passed in May 2000 and came into effect on 17 October of the same year. It sought to criminalize a range of cyber activities including hacking and the publication of obscene information online.<sup>5</sup>

The Act, however, was met with a volley of criticisms, some of them being that it did not contain any provision for protecting children from viewing harmful content on the net, or for protecting individual rights of privacy.<sup>6</sup>

## 1.3.1.2.IT (AMENDMENT) ACT 2008 - TIGHTENING THE STRANGLEHOLD?

The Amendment grants the government wider discretion to exercise censorship.

Firstly, the Amendment has increased the purview of the Act by amending section 2(h) of the Act. The word "computer" has been replaced by the word "communication devices". These communication devices include mobile phones or any other device used to communicate, store and transfer data in the form of text, video, audio or images.

\_

<sup>&</sup>lt;sup>3</sup> Ibid.

<sup>&</sup>lt;sup>4</sup> Jacque deLisle, "Politics and Governance in the People's Republic of China", Newsletter of Foreign Policy Research Institute's Watchman Centre, Volume 16, August 2011, p7

Section 69 of the Act also deals extensively with censorship. Sub Clause (1) of this section empowers the Government to order the interruption of any information through a computer source citing reasons such as 'Sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order and prevention of instigation to commission of any cognizable offence'. Sub clause (2) allows the Controller to call upon any subscriber or persons in control of computer resources for facilities and technical support, to decrypt the information required, while subsection (3) spells out the punishment for the subscriber or person in charge for failure to assist the agency in relation to the function prescribed in Sub Section (2).

<sup>&</sup>lt;sup>6</sup>ArunabhGhosh and NandanKamath, Is Internet Really the Leveller?, India Today, 2002

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

Secondly and most importantly, the section 69 was expanded to include the words 'intercept, monitor and decrypt'. Thus the government by the virtue of powers vested in it by this section can itself intercept, monitor and decrypt any information or cause the subscriber of the computer resource to perform the aforesaid activities and also empowers the government to block sites, a power not enjoyed by the government hitherto and section 69 B empowers the government to collect traffic data.<sup>7</sup>

Looking at the IT (Amendment) Act closely, the following issues may arise:

- Since the ambit of the Act has been widened considerably vide the amendment of section 2, the Government will now have the access not only to computers, but also to a variety of other communication devices like the cell phone.
- The IT amendment act brought about the blocking of sites. The grounds on which the sites have to be blocked are the same as they were for intercepting in the original Act. If the central government is satisfied that it is necessary to block the site keeping in mind the parameters mentioned, it can do so. At the time of writing, no such detailed procedures or safeguards relating to the subject at hand have yet been specified. There is a need to state the procedures and safeguards in detail and produce them on paper as well so as to limit the misuse of this provision and power of blocking by the government.<sup>8</sup>
- •Section 69B empowers the Central or State Government to generate, transmit, collect and store "traffic data" for the purpose of enhancing cyber security and for identification, scrutiny and prevention of spread of contaminant. Here again the legislators have failed to specify the procedures and safeguards subject to which monitoring and storage of traffic data may occur.

## 1.4. INFORMATION TECHNOLOGY RULES 2011

According to Section 3(2) of the Information Technology (Intermediaries guidelines) Rules, 2011, the intermediaries must publish certain rules and regulations and terms and conditions warning users not to publish, modify or update any piece of information which, for instance, Is 'grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; or harms minors in any way'; or'threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or or public order or causes incitement to thecommission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.'9

Any information which falls into any of these categories prescribed under this act, which is known or is made known to the intermediary, must be made inaccessible within thirty six

7,

http://www.mit.gov.in/sites/upload\_files/dit/files/downloads/itact2000/it\_amendment\_act2008.pdf

<sup>&</sup>lt;sup>8</sup>PavanDuggal ,*Mobile Laws*, University Law Publishing Co. Pvt. Ltd., Ed 2011.

<sup>&</sup>lt;sup>9</sup> Information Technology (Intermediary Guidelines) Rules, 2011 as to be published in the GAZETTE OF INDIA, EXTRAORDINARY, PART II, section 3, Sub-Section (i) of dated the 11<sup>th</sup> April 2011

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

hours and must be preserved for upto 90 days for investigation purposes. <sup>10</sup>It thus places greater onus on intermediaries to block any information which they consider harmful. Critics of the Rules stated that the Act clearly targeted bloggers, and thatit will have a bearing on all internet firms which accept user generated content such as Google, Facebook, Yahoo, Rediffmail among others. <sup>11</sup>

The result of this advisory committee was the establishment of the Cyber Crime Investigation Cell which deals with cyber crimes and enforces the provisions given in the Information Technology Act 2011. <sup>12</sup>

## 1.5.CENSORSHIP IN CHINA: LEGAL ASPECT

China is arguably one of the most restrictive countries in the world. The Government in China has passed numerous regulations to control, among other things, online sources of information and free debate. Internet censorship in China started way back in 1993 with the passing of the Temporary Regulation for the Management of Computer Information Network International Connection, which required that 'direct linkage with the internet must go through ChinaNet, GBNet, CERNET or CSTNET'- all state owned Internet Service Providers. <sup>13</sup> Also, harmful information that is either 'subversive' or 'obscene' was forbidden.

In 1994, another regulation was passed- the Ordinance for Security Protection of Computer Information Systems, which gave the Ministry of Public Security the right to investigate and prosecute internet activity. It was confirmed when the Government passed the Computer Information Network and Internet Security Protection and Management Regulations (1997 Regulations). Following 1997, there was a sudden burst of regulations relating to internet censorship. In 2000 alone, six major regulations were passed, namely

- Administration of the Maintenance of Secrets in the International Networking of Computer Information System Provisions
- Interim Procedures on the Regulation and Filing of Online Business Operation
- Regulation on Internet Information Service of the People's Republic of China
- Management Provisions on electronic Bulletin Services on the Internet
- Administration of Engagement by State Council and Internet Sites in the Business of News Publication Tentative Provisions
- Decision of the Standing Committee of the National People's Congress Concerning Maintaining Internet Security (National People's Congress Security Law)

They all sought to regulate information which might 'harm social morals' or threaten 'national integrity and social security'. Disclosure of other information such as 'state, military, or intelligence secrets through the internet' was also banned.

-

<sup>&</sup>lt;sup>10</sup> Section 4 of the Information Technology (Intermediary Guidelines) Rules, 2011 as to be published in the GAZETTE OF INDIA, EXTRAORDINARY, PART II, section 3, Sub-Section (i) of dated the 11<sup>th</sup> April 2011

<sup>&</sup>lt;sup>11</sup> 'Internet Users Not Happy with Internet Rules 2011', The Economic Times, May 16 2011, Delhi <sup>12</sup>http://www.cybercellmumbai.com/

<sup>&</sup>lt;sup>13</sup> Vi L Nhan, 'Media in China: Methods of State Control', The Orator, Volume 1, 2008, pp 36-50

<sup>&</sup>lt;sup>14</sup> Article 6, Interim Procedures for Regulating and Filing Online Business Operations

<sup>&</sup>lt;sup>15</sup> Article 1, Management Provisions on Electronic Bulletin Services on the Internet 2000

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

In 2002, the Interim Provisions on the Administration of Internet Publications was passed which required web portals to monitor information posted on web sites.<sup>17</sup>

In 2005, the Provisions for the Administration of Internet News Information Services was issued which held that it was against the law to 'transmit information on any electronic bulletin service that instigates others to hold any assembly, to form any association or to demonstrate in any unlawful manner; or to organize activities carried out in the name of an illegal non-government organization' 18

## 1.6.GOLDEN SHIELD, OR THE GREAT FIREWALL

The Golden Shield, or the "Great Firewall of China" basically refers to the censorship built into the Chinese internet which primarily targets the movement of information between the global Internet and the Chinese Internet. The Golden Shield project is run by the Ministry of Public Services.

## 1.6.1. LIMITS ON CONTENT

Officially, the project seeks only to censor "superstitious, pornographic, violence-related, gambling and other harmful information." However, in practice, a wide range of political and social topics are censored.

This is hardly surprising, given that the Communist Party views dissent as a threat. Topics such as "freedom of speech" and "human rights" are not as heavily censored, although they are far from uncensored.<sup>20</sup>

## 1.7.MOTIVES AND SOURCESBEHIND THE LAWS

It has been seen from the above information that the motive behind internet censorship in India are mainly to protect the national interests- integrity, sovereignty and unity of the country, relations with foreign states, public order etc. Laws censoring pornography seek to protect social values and norms.

On the other hand, in China, the Internet is seen as a potential threat to the continued leadership of the Chinese Communist Party. It seeks to block any information which may lead to social or political discussion that could disrupt social stability and threaten state security. Only politically correct speech is allowed to be published on the net. Information which is considered harmful to the reputation of the state, anti government content, ideas that undermine state religious policy are removed. Other content which is banned include 'socially harmful material' such as pornography.

<sup>&</sup>lt;sup>16</sup> Article 2, National People's Congress Security Law 2000

<sup>&</sup>lt;sup>17</sup>Article 6, Interim Provisions on the Administration of Internet Publications

<sup>&</sup>lt;sup>18</sup>Article 19, Provisions for the Administration of Internet News Information Services

<sup>&</sup>lt;sup>19</sup>China and the Internet. International Debates, 15420345, Apr2010, Vol. 8, Issue 4

<sup>&</sup>lt;sup>20</sup>Freedom on the Net 2011, Freedom House.http://www.freedomhouse.org/images/File/FotN/China2011.pdf, accessed on 7 October 2011.

<sup>&</sup>lt;sup>21</sup> Anne SY Cheung, 'The Business of Governance: China's Legislation on Content Regulation in Cyberspace', available in www.law.nyu.edu
<sup>22</sup> Ibid

<sup>&</sup>quot;Udgam Vigyati" – The Origin of Knowledge

## 1.8.PROCESS OF IMPLEMETATION OF CENSORSHIP BY THE RESPECTIVE COUNTRIES

This chapter aims at describing in detail the manner in which laws of cyber censorship are implemented in India and India.

# 1.7.1. IMPLEMENTATION OF THE CYBER CENSORSHIP BY THE INDIAN GOVERNMENT

After the ITA amendment act 2008, the Ministry of Communications and Information Technology has got the rights to block and censor any material that might be considered as a threat to national security and also assigning imprisonment for up to seven years for anybody who fails to comply with the rules. This step has been taken in order to provide more rigidity and uniformity and is also much faster than the current existing system, where the system has been decentralized into several monitoring agencies under various ministries.<sup>23</sup>

## 1.7.2. ENFORCEMENT OF CENSORSHIP BY THE CHINESE GOVERNMENT

Policy regarding the actual content is to be censored is mostly directed by the State Council Information Office and the Chinese Communist Party's Propaganda Department, with input from other government and public security organs<sup>24</sup>. The criteria of blocking contents, though prescribed under various articles which govern the internet censorship in China, in practicality is heavily dependent upon the wishes of the government.

The concept of self-censorship also prevails in China. The concept preys on the fears of the civilians who, out of fear of being legally prosecuted by the govt., censor their own content before publishing it online. <sup>25</sup>

## COMPARATIVE ANALYSIS BETWEEN IMPLEMENTATION OF CENSORSHIP LAWS IN CHINA AND INDIA

The process and methodology used for censoring the internet in India and China is pretty similar. Both the countries have rules and regulation in place, which govern the cyber laws. In India, censorship is governed mainly by the IT Act and in China, by a series of laws and regulations as mentioned above. Also there are specialised agencies to govern the internet and enforce censorship laws- the Indian Computer Emergency Response Team (CERT-IN) and the Ministry of Industry and Information Technology (MIIT) respectively. Internet is also filtered through licensing requirements. However, the censoring of content is exponentially higher in China than in India. Any sort of criticism regarding the authoritative heads of China or about the rampant corruption in the system is not accepted and is immediately censored.

 $<sup>^{23}</sup> http://articles.economic times.india times.com/2010-08-18/news/28489522\_1\_cms-telecoms-department-centralised-system$ 

<sup>&</sup>lt;sup>24</sup>Eric Harwit and Duncan Clark, "Shaping the Internet in China: Evolution of Political Control Over Network Infrastructure and Content," *Asian Survey*, 41:3, May-June 2001, pp. 337-408.

<sup>&</sup>lt;sup>25</sup>http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1683823

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

## REASONS FOR DISPARITY BETWEEN THE IMPLEMENTION OF CENSORSHIP LAWS BETWEEN THE TWO COUNTRIES

The root of this difference lies in the 'Doctrine of Separation of Powers', which as has already been mentioned, is widely accepted and acknowledged in India but only another ineffectiveconstitutional provision in China.

In India, the legislature, the executive and judiciary are three separate units of the Government, each with their own realm of powers and functions. At the same time, a system of 'checks and balances' has also been provided forwhich ensures that neither of the organs would exercise its power arbitrarily. For example during the late 1990's , when VSNL denied access to Internet Telephony sites such as Vocal Tec, Net2Phone and Web Phone in order to counter the threat it faced from a VoIP software used to make international calls, Mr.Arun Mehta, a telecom consultant, protested against this ban and challenged VSNL, filing a case against the ISP in the Delhi High Court. <sup>26</sup> The Court ordered the ban to be lifted.

## **Consequences, Pros and Cons**

This chapter will look at the effects these laws have had on the people of the respective countries, the reactions they have elicited, and the manner in which the government deals with it. Also, this chapter will cover the positive and negative aspects of these laws. The positive aspects will include the need for these laws, and the possible ramifications of not having them in place. The negative aspects will look at the abusive implementation of these laws by the government to suppress dissent against their regime.

## 2.1. FIGHTING BACK

In both countries, it has been observed that censorship elicits a largely negative response. People have a tendency of revolting against restrictions and controls imposed on them, and have found ways and means to get across such censorship.

#### 2.1.1. CHINA

Blogging is the new medium through which citizens are voicing their dissent. This can be seen by the rise in the number of blog users over the last few years - about 113 million people update either a blog or personal website on a regular basis. While many of them are shut down or blocked, several manage to get their message across. SinaWeibo, a microblogging application similar to Twitter, has especially grown in popularity since its launch in 2009. As of October 2010, it has approximately 50 million users. <sup>28</sup>

KetanTanna, last accessed on 11/10/11 http://www.ketan.net/INTERNET\_CENSORSHIP\_IN\_INDIA.html 
<sup>27</sup>Freedom House, Freedom on the Net 2011. http://www.freedomhouse.org/images/File/FotN/China2011.pdf

accessed on 8 October 2011

<sup>&</sup>lt;sup>26</sup> Internet Censorship in India: Is It Necessary and Does It Work?

<sup>&</sup>lt;sup>28</sup>http://www.time.com/time/magazine/article/0,9171,2048171-2,00.html accessed on 8 October 2011

#### 2.1.2. INDIA

Reaction to the new IT Rules, 2011 has been overwhelmingly negative. Millions of internet users have spoken out against the new rules, labelling them as 'draconian' and warning that the Indian Government was walking down the Chinese path. Quite a few letters were written to the editors of various newspapers, slamming the new rules. Social networking sites like Facebook and Twitter were flooded with messages speaking out against the new measures. The heaviest criticism came in from bloggers, who were hit hardest by the new rules.

## 2.2. THE TWO SIDES OF CENSORSHIP

While censorship is seen as restrictive and unwanted, there are certain positive aspects of it as well. Censorship to an extent is reasonable. However, it should not be used by the people in power to impose their own views on people governed.

## 2.2.1. NEGATIVES OF INTERNET CENSORSHIP

There are many reasons why the government shouldn't be censoring the Internet. One is that it is a direct violation of Article 19(1)(a) which provides that all citizens have the right to freedom of speech and expression. The fact that the government has full control over what stays on the Internet and what doesn't, gives them the opportunity to take advantage of the situation, which they have done in the past and will in all probability continue to do so. The IT Rules 2011, put the responsibility of policing content on Internet service providers (ISPs), bloggers, Internet companies and just about anyone else managing a website, including social networking sites.

An example of the Government misusing its power was seen in in May 2008, when a tech worker was arrested in Gurgaon for content posted on an Orkut profile "I hate Sonia Gandhi". The government took down the content and gave the IP address to the police, facilitating them in locating his physical whereabouts, and charged him under section 292 of the IPC, which deals with printing of obscene material, and section 67 of the Information Technology Act, which deals with printing obscene material in an electronic form. Neither Google nor the government is ready to openly disclose what was posted but claimed that the material violated India's obscenity laws.

GitanjaliDuggal, Google's in-house litigator in India, believes that what is allowed in print should be allowed online and that mentioning hatred towards a political party is far different from mentioned hatred towards a party due to their religious beliefs. She says that Google pays special attention to anything that may be seen as defamatory because this can lead to libel, which is a criminal offense in India. <sup>29</sup>

In China, censorship is one of the most sophisticated interventions by government. The government's increased efforts are due various anti-corruption and ethnic riots, which were organized via text messages, chat rooms, social networking websites and instant messaging

<sup>&</sup>lt;sup>29</sup>Amol Sharma and Jessica E. Vascellaro, "Google and India Test the Limits of Liberty", The Wall Street Journal, January 4 2010, last accessed on 11/10/11http://online.wsj.com/article/SB126239086161213013.html

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

services. China's alleged Internet police is rumored to have a strength of 30,000.<sup>30</sup> This censorship has faced much critic both inside the country and out.

## 2.2.2. POSITIVE ASPECT OF CENSORSHIP LAWS

On the other hand, there is a positive aspect to cyber censorship also. Cyber censorship does not curb the freedom of speech as such. Rather it is merely draws the line between freedom and unrestrained deviltry.<sup>31</sup> Censorship restricts access to objective and questionable content, which is usually excessively violent or sexually explicit. Where most audiences are ready for portrayal of subjects like sex and violence, there is a level of discretion needed, especially when children are involved, as these shape the morals and values of the child, which will stay with him throughout his life. 66% of children aging 10-17 have seen online pornography without the intention of watching it. <sup>32</sup>

In a country like India, where there is a huge diversity and even the minorities represent a large part of the country, racial or religious discrimination is simply not tolerable. When prophet Mohammad was portrayed in a disrespectful manner on a popular adult cartoon show, South Park, people were outraged and were on the rim of rioting.

Another aspect that needs to be looked into is the fact that most of the users in China believe that the government should have control over the Internet. In a survey by Pew Internet and American Life Project of Chinese Internet users, conducted in 2008, it was found that in 2007, around 85% of the Internet users strongly felt that the Internet should be under the control of the government. <sup>33</sup>

The government's aim, in censorship is not so much to restrict the freedom of speech but is fundamentally to maintain their power and legitimacy. The government is trying to provide a stable government which provides security to the people and the country.

## Legitimacy

Legitimacy of a law can be broadly defined as the acceptance of a governing law as an authority by people being ruled by it. In the context of legitimacy, Friedrich, an American political theorist states that 'the question of legitimacy is a question of fact that whether a given rulership is believed to be in a good title by most men subject to it.' This definition can be used to determine the legitimacy of laws both from the Natural Rights perspective and Positivist perspective. As Austin says that for positivists "the existence of law is one thing; its merit and demerit another. Whether it be or be not is one enquiry; whether it be or be not

http://www.parliament.nsw.gov.au/prod/PARLMENT/publications.nsf/0/3043e49ab3f4abf9ca2573530006f989/\$FILE/Dealing%20with%20Online%20PredatorsFINAL&INDEX.pdf

<sup>&</sup>lt;sup>30</sup> Jonathan Watts, "China's secret internet police target critics with web of propaganda", The Guardian, 14 June 2005, last accessed on 11/10/11

http://www.guardian.co.uk/technology/2005/jun/14/newmedia.china#article\_continue

<sup>&</sup>lt;sup>31</sup>SanayaDadachanji, "Censorship: An Eyewash in India", http://www.mkaco.com/images/censorship.pdf, last accessed 11/10/11

<sup>&</sup>lt;sup>32</sup>Gareth Griffith and Lenny Roth, "Protecting Children From Online Sexual Predators", NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE, last accessed 11/10/11

<sup>&</sup>lt;sup>33</sup>Deborah Fallows, "Most Chinese Say They Approve of Government Internet Control," Pew Internet & American Life Project Report, March 27, 2008, http://www.pewinternet.org/report\_display.asp?r=246

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

conformable to an assumed standard, is a different enquiry" and this clearly captures the essence of positivism which lays emphasis only on following a procedure in order to assess legitimacy of laws and ignored its acceptance by people and whether the provisions fitted in well with the given social conditions.

In this chapter the issue of legitimacy of laws is studied by critically examining and comparing laws on cyber censorship in China and India drawing on examples discussed in the previous chapters.

#### **3.1. CHINA**

In law making body in China, as evident from discussion in previous chapters is the National People's Congress. This legislature organ is the highest law making authority in the country and the members to this group are not democratically elected by people of China. Some of these rights are often human rights enshrined in the constitution of China which are not safeguarded by the judiciary. In the context of laws related to cyber censorship, citizens in China are fine with internet regulations restricting the access of such content which is obscene and could lead to disturbance of harmony in the community.<sup>34</sup> They however are unhappy with regulations that impose unreasonable restrictions on public as is the case in China where political content is censored to great degree. As there is no system of checks and balances between the various organs of the government, the power is heavily concentrated in the hands of the Executive which is supreme and has power to control the decision given by the judiciary. In context of cyber censorship in China, interpretation of relevant laws often legitimises unreasonable censorship of political content y the government which has wide discretionary powers in these matters. This is clearly undermines the legitimacy of the laws coming out from these bodies which are no longer receive acceptance of the public questioning the legitimacy of Government of China.

#### **3.2. INDIA**

In India, if the question is asked – what is legitimate, the answer to it would probably be, nay law of the people, for the people, by the people. Legitimacy in India draws from the consensus of people and their ideas of what is morally right or wrong.

In India, the law making body is the Parliament which is fairly representative of the people. Also, as seen in the first chapter, in India the principle of separation of powers between the legislature and the judiciary is quite functional. The judiciary has the power to declare any law that violates the fundamental rights of the people, null and void.

In India, the sole law governing the cyber space is Information Technology Act. This Act, though having been passed by the parliament, can be annulled by the judiciary to the extent of it being inconsonant with the provisions of the Constitution. The legislature has been fair in designing most of the provisions of this Act. For example, with respect to section 67, the government has given full discretion to the internet service providers to decide what is

<sup>34</sup>Chinese Academy of Social Sciences Beijing, Surveying Internet Usage and its Impact in Seven Chinese Cities, (Center for Social Development,2007) is survey covering internet users in the seven major cities of Shanghai, Guangzhou, Chengdu, Changsha, Xian, Shengyan

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

prurient or laviscous. Leaving it to the discretion of the website controllers will grant a certain degree of room for people to decide in consonance with their own principles, what is objectionable and what is not.

Also, in India, the public spirited individual can file writ petitions in the court for any matter to be reviewed, as it was in the case of Justice Sunil and JayeshThakkar. The Act also allows any person whose rights have been violated by the said Act to appeal to the CAT and an appeal also lies against this tribunal. The only downside to the cyber law situation is the section 69 of the Information Technology Act. This provision as seen in the previous chapters empowers the government to block the sites without prescribing any safeguards and provisions. This provision can be called "unacceptable" as, it has been that the blocked sites are being viewed by using the other internet providers outside India.

## **Conclusion**

The conclusion of the project summarizes what has been said in the chapters and discusses them in the light of personal experiences. It aims at providing a like between all the chapters binding them together to form a seamless and comprehensive whole.

The matters that have been discussed, in short are:

## **CHAPTERS**

#### **CHAPTER 1:**

It provided the bigger picture of the project, i.e the general context for which censorship is discussed as a specific example. The two systems of governance that exist in the countries which are the focus of this project: authoritarian and democratic, in the countries of China and India respectively is a major theme of the project. To recapitulate:

## 1.1. Separation of Powers:

India, there is no specific provision dealing with the Doctrine of Separation of powers. It has only been implied. It is worthwhile to mention that Article 50 provides for a complete separation of the judiciary from the executive.

In practice, however, the separation of powers in India is not *absolute* as powers often overlap. The doctrine has mainly evolved in India through a number of judicial decisions. The constitution also provides a system of checks and balances, which aim at making sure that absolutely no institution gains monopoly over any issue. The system of separation of powers is widely accepted and acknowledged in India.

As the background for the bigger picture has been established, the next section puts forth the specific example of cyber censorship in this light. The law related to cyber censorship has been discussed in detail, including its evolution in both countries, and then consequently the issues stemming from it, such as practicality, drafting, management relations etc have been put forth. To continue, a comparison of these factors in the two countries has been given.

Evidently, there is a disparity in the manner in which these factors play out in the two countries by virtue of the different systems of government.

## 1.2. The Law and issues stemming from it.

Section 3(2) of the information technology (intermediaries guidelines) rules 2011 establishes a fairly exhaustive list of contexts during which cyber censorship can be enforced. It includes publication of material that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever, or that can harm minors in any way, or violates any law for the time being in force as examples.<sup>35</sup>

## IT Amendment Act 2008

In India censorship is mainly governed by the IT Act 2000, its Amendment (2008) and the recent rules passed by the Government- the IT Rules. Article 67 of the original act dealt with porn whereas article 69 empowered the govt to order the interruption of any information through a comp. citing reasons such as integrity, security of the country etc. It was criticised because it was seen as too intrusive and there was nothing to protect children from viewing harmful content on the net as well as a variety of other reasons. There was a need to amend it. The Amendment of 2008 however increased the scope of the govt to exercise censorship by replacing the word comp. with comm..devices in article 2. At the same time 67 was expanded to include child porn.

## Implementation of the Cyber Censorship by the government

The Indian government is partly free with limits on content. While YouTube, Facebook etc have been allowed, the content is still subject to governmental approval and can be removed if thought of as likely to cause damage of any sort. Blogs are rarely censored. The area covered by the IT Act isn't exactly defined. The Centralized Monitoring System (CMS) is being developed to keep checks on traffic that goes past internet, regardless of the network. As in defamation, there exists a fine line between slanderous comment and freedom of speech and expression.

In China, however, the laws are not a specific set that govern the internet censorship in China, but rather are a collective of different rules and regulations that govern and control the people's freedom of expression.

Some of the provisions that specifically deal with the internet in China are Article 23 of regulations, the rule on establishing of cyber cafes, the ban on secrets of Internationally Networked Computer Informations Systems, among many others. Foreign media is heavily restricted, and permission from the government is mandatory for publication.

<sup>&</sup>lt;sup>3535</sup> Information Technology (Intermediary Guidelines) Rules, 2011 as to be published in the GAZETTE OF INDIA

<sup>&</sup>quot;Udgam Vigyati" - The Origin of Knowledge

## **CHAPTER 2:**

Every action has a consequence. These laws obviously effected and elicited a reaction from the people it was intended for – something the governments had to deal with. Do these reactions imply that the laws are an evil? Does the government's reaction imply that this is what's best for the country? The positive and negative aspects of cyber censorship have been elucidated upon.

## 2.1. Fighting back:

People have not been idle, they have been expressing dissent by means of blogging. Statistics reveal that 113 million people update their blogs on a regular basis. Google removed the censorship software that they installed in their search engines on the request of the government after facing a cyber-attack on their data-base.

## 2.2. Positive and negative aspects of censorship:

In China, censorship provides national security, keeps pornography out, and the law, in written form at least, tries not to infringe upon the rights of speech and expression. In India, censorship is at times required to keep riots at bay, and protects women and child rights by banning paedophilia and some forms of porn. These can be said to be the positive aspects.

On the other hand, censorship laws are pervasive, stifle public opinion, and cause violation of user rights. In India, there are instances of the government misusing the law, as is demonstrated in the vague and open-ended law implemented in April, 2011.

#### **CHAPTER 3:**

So far, the law has been discussed only in terms of the difficulties and issues it poses. The third chapter adds the other angle relevant to the course, the one of legitimacy. This chapter poses the most critical question, the one of legitimacy. Is legislation valid based solely on the merit of it having been passed by the law making authority of a country? What weightage must be accorded to the consensus of the people? Cyber law is just an example for laws in general in this chapter. It's symbolic of all laws that come under public scrutiny on account of the varying opinions of their utility.

The third and final chapter discussed the most critical aspect of this law, and will use cyber law as an example to discuss legitimacy and acceptability of laws in general. It brings out the difference between institutional and ideational sources of law and embodies the debate between positivists and anti-positivists (advocates of natural law). It discussed hot rights nowadays are derived from laws, as opposed to them being formulated with the objective of protecting rights.

#### **OPINION OF RESEARCHERS**

The researchers concur that laws of cyber censorship must exist, but should not block more than essential content. While blocking paedophilia and other such content, the authorities must always keep in mind the fact that these laws are drafted to ensure well-being of the people they are meant for, and not for maintaining their position of power. A moderate solution is best, but enforcement of such an ideal system might prove to be impossible.

## **BIBLIOGRAPHY**

- Jacque deLisle, "Politics and Governance in the People's Republic of China", Newsletter of Foreign Policy Research Institute's Watchman Centre, Volume 16, August 2011, p7
- ArunabhGhosh and NandanKamath, *Is Internet Really the Leveller?*, India Today, 2002
- SakshiSawhney, "The Information Technology(Amendment) Act 2008: The Provenance of e-policing", Nalsar Student Law Review, 2010
- Vi L Nhan, 'Media in China: Methods of State Control', The Orator, Volume 1, 2008, pp 36-50
- Anne SY Cheung, 'The Business of governance: China's Legislation on Content Regulation in Cyber Space', available in www.law.nyu.edu
- Anne SY Cheung, 'The Business of Governance: China's Legislation on Content Regulation in Cyberspace', available in www.law.nyu.edu
- http://www.cert-in.org.in/s2cMainServlet?pageid=CHARTMISSION
- http://www.cybercellmumbai.com/
- http://www.cyquator.com/html/vol1.pdf
- http://contentsutra.com/article/419-govt-bans-popular-toon-porn-site-savitabhabhi.com-mounting-concern-over/Media/
- http://www.hyderabadpolice.gov.in/Frauds/CyberCrimes.htm
- http://articles.economictimes.indiatimes.com/2010-08-18/news/28489522\_1\_cms-telecoms-department-centralised-system
- http://www.cecc.gov/pages/virtualAcad/exp/explaws.php
- http://newmedia.cityu.edu.hk/cyberlaw/gp3/pdf/law\_security.pdf/gp3/pdf/law\_security.pdf
   y.pdf
- http://www.nytimes.com/2011/05/05/world/asia/05china.html?\_r=1
- http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1683823
- http://news.bbc.co.uk/2/hi/technology/4645596.stm
- http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc
- http://www.freedomhouse.org/images/File/FotN/China2011.pdf
- Internet Censorship in India: Is It Necessary and Does It Work?
- KetanTanna, last accessed on 11/10/11 http://www.ketan.net/INTERNET\_CENSORSHIP\_IN\_INDIA.html

- Amol Sharma and Jessica E. Vascellaro, "Google and India Test the Limits of Liberty", The Wall Street Journal, January 4 2010, last accessed on 11/10/11 http://online.wsj.com/article/SB126239086161213013.html
- SanayaDadachanji, "Censorship: An Eyewash in India", http://www.mkaco.com/images/censorship.pdf, last accessed 11/10/11
- Gareth Griffith and Lenny Roth, "Protecting Children From Online Sexual Predators", NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE, last accessed 11/10/11
  - http://www.parliament.nsw.gov.au/prod/PARLMENT/publications.nsf/0/3043e49ab3f4abf9ca2573530006f989/
- \$FILE/Dealing%20with%20Online%20PredatorsFINAL&INDEX.pdf
- SrutiChaganti, *Information Technology Act: Danger of Violation of Civil Rights*, Economic and Political Weekly, Vol. 38, No. 34 (Aug. 23-29, 2003), pp. 3587-3588.
- http://www.mit.gov.in/sites/upload\_files/dit/files/downloads/itact2000/it\_amendment \_act2008.pdf
- PavanDuggal , Mobile Laws, University Law Publishing Co. Pvt. Ltd., Ed 2011.
- Eric Harwit and Duncan Clark, "Shaping the Internet in China: Evolution of Political Control Over Network Infrastructure and Content," *Asian Survey*, 41:3, May-June 2001, pp. 337-408.
- http://uk.reuters.com/article/2009/01/05/china-internet-idUKSP36401920090105?sp=true, accessed on 7
- October 2011
- http://rconversation.blogs.com/rconversation/2009/01/chinas-latest-i.html accessed on 7 October 2011
- http://www.msnbc.msn.com/id/28577927/ns/technology\_and\_science-tech\_and\_gadgets/ accessed on 7 October 2011
- http://advocacy.globalvoicesonline.org/2009/06/08/china-green-dam-pc-filtering/accessed on 7 October 2011
- http://www.pcworld.com/article/145302/has\_chinas\_green\_dam\_burst.html accessed on 8 October 2011
- http://www.cpj.org/news/2005/China07sept05na.html, accessed on 8 October 2011
- http://arstechnica.com/news.ars/post/20060512-6823.html , accessed on 8 October 2011
- Clive Thompson, "Google's China Problem," New York Times Magazine.
- http://googleblog.blogspot.com/2010/01/new-approach-to-china.html, accessed on 7 October 2011
- Hong Kong Basic Law, Chapter II, Article 18
- http://news.bbc.co.uk/2/hi/asia-pacific/8582233.stm accessed on 7 October 2011