
CENSORING THE INDIAN CYBERSPACE

2006 WHITE PAPER PREPARED BY
MISUM HOSSAIN, VICE PRESIDENT
GLOBAL SCHOOL OF TECH JURIS

Censoring the Indian Cyberspace

The Indian Cyberspace has seen a sudden yet not surprising growth of curiosity and interest among students, professionals and organizations from a diverse range of sectors. Although the menace of cyber crime has been unnoticeably gnawing away in India for quite some time now, the interest that it has generated in the recent past has been quite remarkable.

The unprecedented concern about cyberspace and the governing laws can be attributed to a number of reasons. The media has made a significant contribution to this cyber awareness by identifying cyber crimes as an area that requires immediate attention. Another encouraging development has been the proactive methods deployed by Cyber Crime Police Cells across different states in the country. The law enforcement agencies in India have recognized that they will soon be encountering an increasing number of high tech as well as low-tech cyber abuses in the near future. Governments have already started investing in manpower with superior technical knowledge as well as providing funds to the Cells for computers and software tools integral to the aspect of investigation and forensics. Another development that seems to have propelled interest in the issues of cyberspace is the discovery of the discouraging trend that the increase in number of cyber offences perhaps is linked with major criminal incidents and terrorism across the country as well as abroad. Cyber crime investigators around the world are analysing and scrutinizing possible links between the cyberspace and global terrorism. It is a common misconception to quarantine the theme of cyber crimes to only incidents related to

hacking, online frauds, cyber pornography and the likes. However cyber crime today is not limited to just computer activity, major incidents around the world including bomb blasts and terrorist attacks are linked to Internet communications and there is a possibility that seeds of these atrocities could have very well been planted in the cyberspace probably in some innocuous chat room or in a seemingly frivolous email. The cyberspace is being reported to be the favourite channel for covert communications especially because of its tremendous potential for anonymity.

It is important to remember that the roots of the Internet sprouted because of the human need for better communication. Today the Internet is the first choice for those looking to communicate faster and economically. Even though the traditional mediums have not ceased to exist, the Internet and the World Wide Web have transcended the physical parameters of the world and created a virtual platform for communication. However this surge of mobility in communications has created concerns for law enforcement agencies as the same channel once perceived to be a stepping-stone in human communications today has allegedly become an anonymous conduit for offenders.

The cyberspace and its independence has been a matter of concern for several governments although for different reasons thereby bringing about the need for regulating and formally governing the cyberspace. A number of governments have been criticized for scrutinizing the cyberspace and restricting the Internet. As far as India is concerned, it has continued to have a very liberal approach different from its neighbours who have seen it mandatory to control the cyberspace. However the recent phase of events with

media reports in July 2006 claiming that Indian Internet Service Providers had been instructed by the Department of Telecommunication (DOT) to block several Blog sites and domain names can be seen as the first major initiative in an attempt to establish control over the Indian cyberspace [1]. It cannot be ignored that this kind of censorship can create and possibly did create problems for legitimate users. A more potent question is possibly whether blocking this handful of sites is really going to make a difference to covert terrorist communications? The supporters of the Blog community will obviously choose to differ. It cannot be ignored that terrorist cells could very well be communicating through blog sites and chat rooms under the guise of innocuous cyber chatting. But a very serious query seems to be that when these channels are under the scanner, is it advisable to undertake such measures just after the Mumbai blasts, which undoubtedly would alarm the cells into changing their paths in the virtual world. More importantly will this lead to newer modes being discovered for covert communications?

The decision to instruct Indian ISPs to block certain sites has encountered widespread criticism as it is seen as a move towards cyber censorship [2]. However such control is not entirely alien from a global perspective. The Chinese government has found it mandatory to regulate and govern their cyberspace by restricting, blocking and controlling content providers and service providers in the Chinese cyberspace. A prime example of this is Google [3], who have been widely criticized for ingratiating Chinese cyber economy by introducing google.cn, a filtered and greatly curbed version as opposed to its popular incarnation. For the backers of Net freedom, google.cn is a distressing compromise of cyber independence. Even MSN China [4] launched by

Microsoft in 2005, puts restrictions with regards to what Chinese bloggers can write about. Several words have been banned by MSN China and bloggers using these words in blogs or posting obscene messages get automatic warnings from the site requesting users to delete objectionable content. In Saudi Arabia, websites that dent religious sentiments and attempt to propagate blasphemy are blocked. The Indian scenario has hardly reached that stage but it does no harm speculating what would happen if such censorship, although unlikely, were to happen. The recent instance of ISPs blocking sites is definitely not the first attempt in censoring the Indian cyberspace as previously a Yahoo discussion group [5] was banned for alleged links with separatists and for containing material condemning the national as well as the state government in Meghalaya. The site was reportedly blocked after Yahoo officials in India had refused to remove the content from the site [6]. The prohibition resulted in the blocking of all discussion groups hosted by Yahoo in India although a majority of the groups had nothing to do with the offending content. As Indian Internet service providers lacked the technology to ban sub-groups, the blocking of the Internet Protocol Address of the allegedly aberrant group resulted in the blocking of all other discussion groups hosted on the same IP. The essential issue that arises from such gagging orders whether it is the banning of the Yahoo discussion group or the blocking of certain blog sites and web pages is the inconvenience caused to the legitimate users of technology. However an interpretation of the current Indian cyber laws will reveal that the ISPs are trading on thin legal premise.

The answer for the legitimate users lies in the Indian cyber laws or more specifically The Information Technology Act, 2000. Bloggers or site users all around the country,

distressed and disconcerted due to the recent phase of events, do have a legal remedy. It needs to be understood that no regulating or governing body can arbitrarily or randomly block websites without any specific rationale. In the absence of any precise logic behind any online blocking, those at the receiving end like the thousands of legitimate users can hope to get compensated in a court of law from the ISPs. The global condemnation for such capricious action would undoubtedly relegate the Indian cyberspace into a cyber pariah and jeopardise its immense e-potential. It is not surprising that the ISPs have now become the prime target as the government claims that the blocking of blog sites and certain parent sites in July was in contravention of the original order that was communicated to the ISPs instructing them to block certain anti-national websites and webpages.

As far as the bloggers and those others affected by the blocking are concerned, they are more interested in the redressing of their grievances through petitions in a court of law. This brings us to the significant question of whether the Indian cyber law provides an unambiguous explanation for such denial of access. Section 43(f) of The IT Act, 2000 categorically penalizes this kind of unauthorized denial of access and provides the opportunity for each legitimate user to gain compensation of up to Rs. 1 crore.

Bloggers willing to take up the fight are registering with the government's CERT-IN (Computer Emergency Response Team India) but in order to be eligible for compensation, those affected will also have to establish the quantum of their respective losses resulting due to the alleged unauthorized blocking. The success of the bloggers

will most definitely open the floodgates for future petitions from affected individuals demanding compensation for unreliable and irregular services on the Indian cyberspace. Such assurance from the judiciary will inevitably render ISPs and network service providers transparent and answerable to questioning consumers. However censorship, although scrutinized and perceived as a repressive response to unchecked online activity, should be practiced moderately thereby ushering in a period of “regulated cyberspace”. It needs to be understood that the freedom of speech and the independence that the cyberspace provides should at no point of time be abused or manipulated. As there can be no guarantees about ethical online behaviour but at the same time users need to be given freedom, the only solution available in this regard is that of taking certain steps to regulate cyber conduct.

The current trend of blocking blog and websites is less of a measure aimed at harnessing the Indian net users and more of a hastened step in retaliation to the spate of terrorist activities in the nation. Regulation is necessary but it has to be incorporated in a specific manner with definite objectives.

The Department of Telecommunications (DOT) has shown interest in certain sites and the ISPs have complied with instructions but what about regulating the content that thousands of Indian net users are innocently subjected to every day. The Indian cyberspace needs to be properly governed so that citizens can surf safely without the risk of being exposed to potentially dangerous, obscene, or illegal content and hence incurring unwanted liabilities. Advocates of cyber freedom claim that users can control what they

witness by modulating Internet browser behaviour and hence it is the responsibility of a surfer as to what kind of content is visible on the desktop. However it is common for unsuspecting surfers to be faced with obscene options whether through obnoxious pop-ups or while searching apparently innocuous words or phrases through popular search engines. The probability of objectionable sites returning as popular hits as a response to keyword searches is not uncommon but the peril is that the user initiating the search might not be mature enough to distinguish between a site that holds the answer he/she seeks and the one that is there to commercialise products or services that are illegal in India. The solutions to this multitude of problems are not simple and clear-cut nor are they always practical and commercially viable. To add to the woes of cyber supervisors, there are sites providing tools of unauthorized access and hacking, pages tutoring on creating viruses and worms, chat rooms wooing adult content or inciting violence and unpatriotic fervour. The recent discovery that anti-national associations could be using tools of the cyberspace to communicate is just another cog prompting swift transition towards censorship or stringent regulation of the cyberspace.

Although cyber censorship or more precisely regulation is probably a premise that heralds a potentially safer cyberspace, the very notion of chastising the virtual world can lead to the Indian cyberspace being relegated to an outcast. However the question that requires an urgent response is whether the government by imposing restrictions buttressed by the logic of protecting the Indian cyberspace are breaching the fundamental rights guaranteed under Part III of the Constitution of India namely Freedom of Speech and Expression under Article 19(1)(a). The pivotal theme of this writing is the thin line

that juxtaposes cyber censorship and cyber freedom. The Indian courts will perhaps provide a clearer picture as to whether such blocking is indeed amounting to breach or the restriction imposed by the government is in fact reasonable. The grounds of restriction are public order, morality, decency and security. Does the government restriction strike a balance between the freedom guaranteed and the social control permitted by Clauses 2-6 of Article 19(1) of the Constitution of India? The limitation imposed on a person in the enjoyment of a right should not be arbitrary or excessive in nature. Is the censorship of the Indian cyberspace a desperate attempt to look effective amid global cyber terrorism? Or are the measures concerted efforts to regulate the cyberspace? We will not have to wait long for answers as the combustible issues have already been raised and it is just a matter of time when the courts of law in India distinguish arbitrary action from legitimate regulation.

Bibliography

- [1] <http://timesofindia.indiatimes.com/articleshow/1778896.cms>
- [2] <http://www.ciol.com/content/news/2006/106073102.asp>
- [3] <http://news.bbc.co.uk/1/hi/technology/4645596.stm>
- [4] <http://news.bbc.co.uk/1/hi/technology/4088702.stm>
- [5] http://news.bbc.co.uk/1/hi/world/south_asia/3148288.stm
- [6] http://news.com.com/India+bans+a+Yahoo+group/2100-1028_3-5081021.html

The entire contents (c) 2006 Misum Hossain. All Rights Reserved. Prior written permission is required from the author before this publication may be reproduced in any form. The information included in this White Paper has been obtained from sources the author believes are reliable. However this White Paper is for general information only and hence should not be considered as a substitute for advice covering any specific issue. Readers of this publication should seek appropriate professional advice before taking or refraining from taking any action in reliance of any information contained in any part of this White Paper. Neither the author nor Global School of Tech Juris (GSTJ) either expressly or impliedly warrants the accuracy of such information. Please note that the author has taken all reasonable care while preparing the instant White Paper but in case errors and omissions occur, neither the author nor GSTJ will be liable for the errors, omissions or inadequacies of the information or for any interpretations of that information. It is clarified hereby that neither the author nor GSTJ will in any way be held liable for any direct, indirect, special, incidental or consequential damages arising out of the use of the content in this White Paper. Opinions expressed herein this White Paper are solely and exclusively of the author, which are subject to change without notice but at no point of time can they be attributed to GSTJ.
