# INDIANCIVILS *Sample Material*

## CONTENTS

# SOCIAL NETWORKING SITES AND CHALLENGES TO INTERNAL SECURITY

***Sample Material***

Social network sites are web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.

While we use the term "social network site" to describe this phenomenon, the term "social networking sites" also appears in public discourse, and the two terms are often used interchangeably. We chose not to employ the term "networking" for two reasons: emphasis and scope. "Networking" emphasizes relationship initiation, often between strangers. While networking is possible on these sites, it is not the primary practice on many of them, nor is it what differentiates them from other forms of computer-mediated communication (CMC). What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks.

The internet has become an integral part of modern living. The spread of social media and the use of platforms is changing the way society operates. Collectively called Web 2.0 social Media is highly effective as a connection and mass communication tool.

Because social media can be defined, among other things, as tools; how they are used, by whom they are used and for what reason can represent either a threat or an opportunity for national security.

1. Social media itself shouldn't be seen as a potential threat to national security but those who use these tools may pose a potential risk.
2. "It is now a given that social media environments are important sources of data for Understanding the dynamics of the diffusion of information and human behaviour".
3. Evidence suggests that social media had an impact on events such as civil unrest (The Iranian Green Movement and the Arab Spring uprising are good examples).

## How terrorists could use Twitter and Facebook:

Social media is being used for spreading terrorism and drug trafficking but the government is unable to take action because identity of perpetrators of such acts is not known. Take drug trafficking, take terrorism. There are lot of illegal things that is happening through social media. If the identity of such user is known to the government, it is unable to act as the user is often not within the jurisdiction of India.

Hence government recently emphasized that there should be distinction between privacy and anonymity. Once you are able to make that distinction and once you are able to enforce that the identity of the person at least authenticated to the platform that he is on, a lot of these problem specially the one that we saw the migration of people of north east from various cities, would have been taken care of.

Migrant workers fled the north eastern states of India following threats from SMS's and various forms of social media. India accused Pakistan of spreading panic via the use of modified images to spread fear within the tensed states. These were originally images of victims of cyclones in Myanmar that were doctored to give an impression that violence in North eastern states were escalating. India cited 76 Pakistan based websites bearing such images. Offending websites bore Pakistani internet protocol (IP) addresses but could not be directly linked to the state. While such sites that hosted doctored images were traceable, the source of intimidating SMS's proved to be much greater challenge. India had difficulty verifying the source of mass SMS threats and had to impose an overarching ban on bulk text messages to prevent further intimidation of those in north eastern states. In a country that feverishly believes in freedom of speech the use of such measures was a clear sign of desperation. The cost of this exodus was high .the 30,000 people that fled the cities of Bangalore and Mumbai also signalled a massive drop in productivity and economic output. Most of those that fled were migrants. The affected region is an important economic hub having been often termed as silicon-valley of India. Despite the massive search for perpetrators of this cyber-attack, only 8 were apprehended in Bangalore. The community needs to build a consensus to resolve issues related to social media by collaborating with each other and not by just making rules and regulations.

**India and Social Media:** The current edition of the study provides social media usage & behaviour of individuals from Urban India. As per the findings, of the 80million Active Internet users in Urban India, 72% (or 58 Million individuals) have accessed / used some form of social networking. They may have accessed social media using a personal computer (PC), laptop or even a mobile device, as the illustration suggests. Social Media usage ranks only after Email (80%) in terms of usage. Essentially, social networking often serves to be among the "First Internet Uses" of Internet in India i.e. besides the usual reasons like Email, Music and Gaming. Social networking through mobile phones is an ever increasing phenomenon observed today. With mobile penetrations reaching very high levels, and an increasing number of individuals owning feature-rich phones or even smartphones that allow Internet access, social networking is rapidly penetrating the India Active Internet user base. Affordable mobile Internet plans additionally serve rising usage levels.

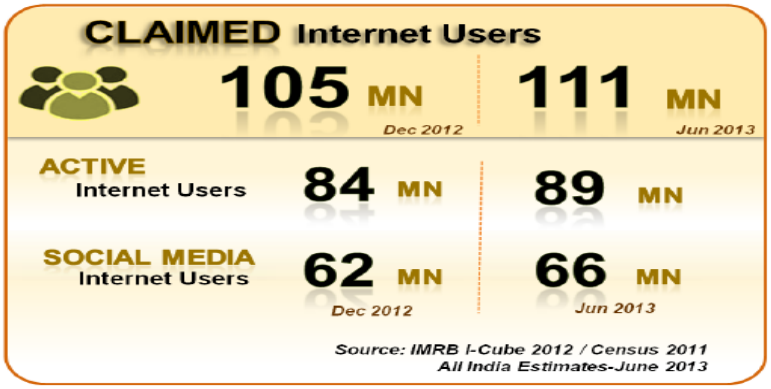


Figure 1 – Urban India Internet Landscape

## How terrorists use the social networking sites for their benefit?

1. Real time updates of troop movements.
2. An operative with a suicide belt can send images to a second operative of his location for an accurate detonation.
3. A cyber terrorist hacks a soldier's account and communicates with other soldiers.

**Purpose:**

1. Terrorism
2. Criminality
3. War
4. Protest and Movements.

In May 2010 the Queensland Police Service began a trial into social media with various objectives such as to develop an online community of followers before a disaster occurred, in light of international examples such as the Mumbai Terrorist attacks. But they found out that though social media dominated the main stream media in Mumbai but the authorities couldn't contribute or manage it with their own social media presence.

## Social media and data analysis

Social media is an important class of big data for analysis as intelligence agencies can measure and understand the millions of people arguing, laughing, joking, and talking, condemning and applauding. The advent of social media sites has created an environment of greater connection among people, businesses, and organizations, serving as a useful tool to keep in touch and interact with one another. These sites enable increased information sharing at a more rapid pace, building and enhancing relationships and helping friends, co-workers, and families to stay connected. Persons or groups can instantaneously share photos or videos, coordinate events, and/or provide updates that are of interest to their friends, family, or customer base. Social media sites can also serve as a platform to enable persons and groups to express their First Amendment rights, including their political ideals, religious beliefs, or views on government and government agencies. Many government entities, including law enforcement agencies, are also using social media sites as a tool to interact with the public, such as posting information on crime trends, updating citizens on community events, or providing tips on keeping citizens safe.

Social media sites have become useful tools for the public and law enforcement entities, but criminals are also using these sites for wrongful purposes. Social media sites may be used to coordinate a criminal-related flash mob or plan a robbery, or terrorist groups may use social media sites to recruit new members and espouse their criminal intentions. Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity. To ensure that information obtained from social media sites for investigative and criminal intelligence-related activity is used lawfully while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, law enforcement agencies should have a social media policy (or include the use of social media sites in other information-related policies). This social media policy should communicate how information from social media sites can be utilized by law enforcement, as well as the differing levels of engagement—such as apparent/overt, discrete, or

covert—with subjects when law enforcement personnel access social media sites, in addition to specifying the authorization requirements, if any, associated with each level of engagement. These levels of engagement may range from law enforcement personnel "viewing" information that is publicly available on social media sites to the creation of an undercover profile to directly interact with an identified criminal subject online. Articulating the agency's levels of engagement and authorization requirements is critical to agency personnel's understanding of how information from social media sites can be used by law enforcement and is a key aspect of a social media policy.

## Social Networks and election campaigning

President Obama's re-election campaign team using automated social media collection to both organise and directly message prospective voters on an unprecedented scale. A recent report indicated that the impact of social media on the next parliamentary election in India would be significant. Sponsored by the Internet and Mobile Association of India and conducted by IRIS Knowledge Foundation, the study contends that the outcome in 287 seats out of India's 543 parliamentary seats would be influenced by the discourse on social media, Facebook specifically. The study juxtaposed the number of Facebook users in each parliamentary constituency with the margin of defeat or victory in the last parliamentary poll in 2009. Based on the differential, constituencies were categorised as High Impact, Moderate Impact, Low Impact and No Impact – in so far as the impact of Facebook is concerned. High Impact seats are those where the numbers of Facebook users are more than the margin of victory. Moderate Impact, Low Impact and No Impact are graded accordingly. Close to half the seats – 256 to be precise – have been termed No Impact constituencies. Predictably, constituencies that the study says will be impacted by the social media are urban seats while the No Impact constituencies are those that are among the poorest in the country.

While the results of the study cannot be ignored, especially by the political class, depending too much on Facebook, Twitter and other social media sites to secure votes would be repeating the mistake made by the Bharatiya Janata Party in 2004. Back then, its leaders mounted a television-centred electoral campaign believing that winning TV debates was all that mattered in politics and votes would come naturally thereafter. In terms of its poverty indicators, India presents the peculiar spectacle of a fall in absolute numbers of the poor while registering an increase from 22 percent in 1981 to 33 percent in 2010. One does not need knowledge of missile technology, on which India has significant spending, to unearth that those live in such abysmally poor conditions have no understanding of the world of social networking.

Even in the 'Impact' constituencies, it would be politically myopic to make political calculations and draw campaign strategies solely by focusing visibility on social media. In most urban constituencies also, the extent of urban poverty is acute and for those who live on the fringes of humane existence social media has little recall value. Data is cited to contend that India, which has currently around 66 million social media registered users is bound to see this number rise to 80 million by the time polls in India are likely to be held in mid-2014. Indian voters are poised to swell up to the 800 million mark by the next hosting's thereby meaning that 10 out of every 100 Indian is a user of social media. But then these 10 do not speak to the 90 others, but they primarily make 'friends' within the elite group. Moreover, even regarding the numbers of registered Facebook users, there is an anomaly. For instance in the Thane constituency adjoining Mumbai, there are 400,000 registered social media uses while the total number of electors in 2009 was 1,800,000. On the face of it, at 25 per cent of the

electorate, Facebook users are an impressive number. But therein lies the larger story that unless accompanied by overall economic uplift, users of technology – both hardware and software – is reaching the saturation point.

There is also the issue that all registered users of Facebook are not regular users. A significant number of those who have registered have rarely lasted more than a few visits but information pertaining to them and their traits has become open secret after the data has been harvested. Making formulations on likely electoral behaviour on the basis of such questionable figures belittles the political acumen of the Indian voter.

Campaign techniques have evolved constantly from the first parliamentary poll in 1952. The one for the next House will also witness a huge blitzkrieg which would be lapped up by the media, especially television channels because its consumers would believe that they are shaping India's destiny. But there is a lot of India that is outside the realm of the social media which is silent and whose responses never surface in the run up to the polls because the media rarely reaches out to them. Facebook, Twitter and other social media sites would give fuel to the evening discussions of the chatterati, but the poll outcome will resonate with the lot of teeth gnashing that is ignored because it carries with it uncomfortable reality of large tracts of India.

## Social media intelligence (SOCMINT)

1. Facebook has been used to organise contract killings, boast about serious animal abuse, and conduct cyber-stalking, plan sexual assaults, breach court orders and cause distress through anti-social 'trolling'.
2. "Government needs to evolve and strengthen SOCMINT capabilities. An independent expert scientific and industrial advisory panel and SOCMINT centre of excellence should be established."

Post-modern terrorists are taking advantage of the fruits of globalization and modern technology – especially the most advanced online communication technologies – to plan, coordinate and execute their deadly campaigns. No longer geographically constrained within a particular territory, or politically or financially dependent on a particular state, they rely on advanced forms of communication - including the Internet. The Internet has long been a favourite tool for terrorists. Decentralized and providing almost perfect anonymity, it cannot be subjected to controls or restrictions, and anyone can access it. The Internet has enabled terrorist organizations to research and coordinate attacks, to expand the reach of their propaganda to a global audience, to recruit adherents, to communicate with international supporters and ethnic Diasporas, to solicit donations, and to foster public awareness and sympathy for their causes. The Internet also allows terrorists to convey their messages to international and distant audiences with whom it would otherwise be difficult to communicate. The Internet provides a means for terrorist groups to feed the mass media with information and videos that explain their mission and vision. Thereby, the group's message can reach a greater audience and more easily influence the public agenda.

In addition to launching their own websites, terrorists can harness the interactive capabilities of chat rooms, instant messenger, blogs, video sharing websites, and self-determined online communities and social networks: These forums act as a virtual firewall to help safeguard the identities of those

who participate, and they offer subscribers a chance to make direct contact with terrorist representatives, to ask questions, and even to contribute and help out the cyber terrorism.

By now, all active terrorist groups have established at least one form of presence on the Internet and most of them are using all formats of up-to-date online platforms - e-mail, chat rooms, e-groups, forums, virtual message boards, and resources like You-Tube, Facebook, Twitter, and Google Earth. This report examines the use of interactive online communication by terrorists and their supporters – from chat rooms to Twitter Facebook.

**Terrorist Chartrooms**

Chat rooms and electronic forums enable terrorist groups to communicate with members and supporters all over the world, to recruit new followers and to share information at little risk of identification by authorities. In addition to being used to generate support, chat rooms are used to share tactical information. Terrorist message boards and chat rooms have been known to have "experts" directly answer questions about how to mix poisons for chemical attacks, how to ambush soldiers, how to carry out suicide attacks and how to hack into computer systems.

**When Terrorists "Tweet"**

An intelligence report released in October of 2008 by the Army's 304$^{th}$Military Intelligence Battalion included a chapter entitled the "Potential for Terrorist Use of Twitter," which expressed the Army's concern over the use of the blogging services. The report says that Twitter could become an effective coordination tool for terrorists trying to launch militant attacks. The Army report includes references to several pro-Hezbollah Tweets. The report also highlights three possible scenarios of terrorist usage of this online format. The first scenario is that terrorists can send and receive near real-time updates on the logistics of troops' movements in order to conduct more successful ambushes. The second is that one operative with an explosive device or suicide belt uses his mobile phone to send images of his or her location to a second operative who can use the near actual-time imagery to time the precise moment to detonate the explosive device. The third is that a cyber-terrorist operative finds a soldier's account and is then able to hack into his account and communicate with other soldier's under the stolen identity. Although the last two options seem a bit far-fetched and difficult for terrorists to carryout successfully, the first option is a very viable threat. The instantaneous update capabilities could help the terrorists organize more precise and detrimental ambushes.

**Social networking**

Popular social networking websites are another means of attracting potential members and followers. These types of virtual communities are growing increasingly popular all over the world, especially among younger demographics. Youths are especially targeted for propaganda, incitement and recruitment purposes by terrorist groups. Predominately-Western online communities like Facebook, MySpace and Second Life and their equivalents are being used more and more by terrorist groups and their sympathizers. Social networking websites allow terrorists to disseminate propaganda to an impressionable age bracket that might empathize with their cause and possibly agree to join.

Many users join interest groups that may help terrorists target users whom they might be able to manipulate. Many social network users accept people as friends whether or not they know them, thereby giving perfect strangers access to personal information and photos. Some people even

communicate with the stranger's and establish virtual friendships. Terrorists apply the narrowcasting strategy to social networking sites as well. The name, accompanying default image, and information on a group message board are all tailored to fit the profile of a particular social group. The groups also provide terrorists with a list of predisposed recruits or sympathizers. In the same way that marketing groups can view a member's information to decide which products to target to your webpage, terrorist groups can view people's profiles to decide whom they are going to target and how they should configure the message.

**You have a friend request: Facebook**

Membership within the international Facebook community has boomed in recent years. Facebook is currently the world's most popular social networking website. Terrorists have taken note of the trend and have set up profiles as well. There are numerous Facebook groups declaring support for paramilitary and nationalist groups that the U.S. Government has designated as terrorist organizations, such as Hezbollah, Hamas, the Turkish Revolutionary People's Liberation Army and the Liberation Tigers of Tamil Eelam. The majority of these groups have open pages and anyone interested can read the information, look at the discussion boards, clink on links to propaganda videos and join the group.

**YouTube**

The uploading, downloading and viewing video tapes and segments has become very popular. YouTube was established in February 2005 as an online repository facilitating the sharing of video content. YouTube claims to be the "the world's most popular online video community." A 2007 report from the Pew Internet and American Life Project, which put the percentage of US online video viewers using YouTube at 27%, ahead of all other video sharing sites. In the 18 to 29 year old age groups, this leadership is even more pronounced with 49% of US online video viewers using YouTube.

Terrorist groups realized the potential of this easily accessed platform for the dissemination of their propaganda and radicalization videos. Terrorist's themselves praised the usefulness of this new online apparatus: "A lot of the funding that the brothers are getting is coming because of the videos. Imagine how many have gone after seeing the videos. Imagine how many have become martyrs," convicted terrorist testified. The internet has become a central part of modern life. And the spread of social media - blogs, web forums, chat sites and media-sharing platforms (often collectively called Web 2.0) - is changing how societies operate. These tools are also attracting attention from national security planners. In the United States, security and intelligence agencies are exploring the potential of social networking tools for diplomatic, military and homeland security applications. The US State Department has more than 600 social media accounts to inform and interact with international audiences. And the Federal Bureau of Investigation has sought private-sector assistance to develop new software to mine social networking sites to predict future trends and identify possible threats.

The future of armed conflict will be influenced by social media and today's shift towards mobile devices and higher broadband speeds is accelerating these trends. Such changes are said to be just as significant, perhaps more so, than any previous "revolution" in military affairs. As a source of instant information, social media can be exploited by governments to provide greater situational awareness to military commanders, diplomats and aid workers during periods of heightened tension and conflict.

Knowing the "mood" of the enemy through crowdsourcing or data mining may prove to be decisive in battle. But social media is outside state control and it doesn't discriminate. The Iranian Government's use of the same social networking tools to harass, identify and imprison the Green Movement protesters in 2009 showed that the internet can have positive and negative effects.

Terrorist organisations, including al-Qaeda, regularly use social media websites like YouTube and Facebook to disseminate propaganda to a global audience. Their aim is to reach out, recruit and radicalise. Web forums and chat rooms now play a critical role in terrorist communication networks. With near unfettered access to the digital world, terrorists are using the advantages of social media in ways that governments have yet to fully appreciate. The adoption of social media across the Australian national security community has not been consistent or without controversy. Many agencies ban individuals from using Facebook, Skype and Twitter. Concerns over privacy and confidentiality have led to restrictive practices. The capacity of governments to exploit Web 2.0 applications for national security purposes remains unclear.

The review of intelligence community observes that military commanders will increasingly require intelligence agencies to provide an understanding of the human terrain. To achieve this, a clearer national strategy is needed to manage the expanding "ocean" of electronic data, including open-source information available through social media. Proponents of social media demand they do more; sceptics continue to caution against progressing too quickly. In a world of "global listening", a higher premium will be placed on the ability of intelligence agencies to sort the background chatter from critical information. Many advocates of social media argue that governments will need to be active participants in shaping these global debates, and not just active listeners.

As the recent United States Defence Advanced Research Projects Agency research on strategic communication has acknowledged, this will require new methodological tools that employ a creative mix of both social science and technology. The debate over social media and national security is still in its infancy. Further research is needed to understand how social media tools can be integrated into war fighting and diplomacy, exploited for intelligence purposes, and improved upon. New analytic tools, utilising both social science and hard science applications to measure linkage patterns and content in new media, offer some hope of bridging this gap.

Understanding the role of networks - either online or in person - is an increasingly critical task in dealing with a range of national security challenges from combating terrorist groups to responding to natural disasters. If social media tools can assist in those tasks, then the Government should learn to embrace them.

## NATIONAL SECURITY AND THE INDIAN MEDIA: An Analysis

The Indian media in relation to coverage, discussion and analysis of India's national security matters has displayed a deplorable insensitivity to both national interests and national security interests. In this respect the electronic media is more to blame with their attempts to encapsulate complex national security issues into thirty second sounds "bites" so says Michael J O'Neill, former President of the American Association of Newspapers Editors.

**The Indian Media- See The Mirror:** This author had earlier written a piece on "National Security and Indian Media Imperialism" (www.saag.org/papers3/paper214.htm) to highlight how the Tehelka

tapes, motivated by considerations other than noble, affected national security. So before the views in this paper are dismissed as biased, let me quote experts in original from a paper entitled "Developing Preventive Journalism" by Michael J O'Neill.Michael O' Neill's observations given below serve a good purpose as they enable holding a mirror to the Indian media and enable it to introspect:" It is well known that media are more devoted to conflict than to tranquillity, and that war is routinely defined as news, while peace is not. What is good for the world, in other words, is not necessarily good for the news business" Michael O'Neill further lists six phenomenon which are especially relevant and need to be focused on when the media fraternity introspect a change.

These six phenomenons are:

1. "Persistence of the journalistic tradition that is superficial, poorly informed and essentially reactive."
2. Lack of media self-censorship or control as a result of information and news explosion, and emergence of multiple outlets and activist reports.
3. A sharp cutback in the number of foreign correspondents.
4. "Wildfire spread of new technologies that on the one hand are democratising communications but on the other hand are neutering the journalist gatekeepers who traditionally apply standards of accuracy and balance to protect the public against dangerous distortion of news.
5. Destructive and invasive influence of journalism
6. High cost of preventive journalism that profit chasing multi-media and chain owned newspapers are unwilling to pay.

The above observations though pertinent, may be dismissed by the Indian media fraternity as observations made in the American context. But they are pertinent as the Indian media itself attempts to adopt the Western templates not recognising that India's national security environment and political and social milieus are different.

**An Indian Journalist Holds the Mirror to the Indian Media:** However to assuage their feelings, and holding the mirror aloft to see their own shortcomings, let me quote one of their own fraternity.

**India's National Security Issues and Indian Media Record:** Limitations of space preclude a detailed expose and hence only some main issues can be highlighted on a case by case basis as follows:

- **India's Nuclear Weapons Test 1998:** The Indian media went berserk in politicising the issue. It chimed that there were no national security threats in evidence justifying it. Within seven months the Kargil War took place.
- **Pakistani Proxy War in J&K:** The media has been totally irresponsible. India's strategic sensitivities are constantly ignored and there is a competition to adopt extreme liberalist views. One theme often stressed is of Kashmiri alienation. Had that been so, Pakistan by now would have inflicted a Bangladesh on India.
- **Kargil War:** Instead of marshalling the nation into a cohesive force, the Indian media playing partisan political roles at the height of the war, were busy stoking controversies as to how it happened.

- **Agra Summit:** The summit had more to do with India's national security interests than political diplomacy. The Indian Media went berserk in focusing and projecting General Musharraf's view point than advancing India's interests. What a comparison to the Pakistani journalists who utilised India's electronic media space to defend and advance their country's interests.
- **India's Military Mobilisation December 2001:** Pakistan did not have to use ISI to spy on India's mobilisation efforts and moves of its strategic formations. The Indian media was doing the job.

**Indian Media Needs to be reined in on National Security Issues:** The stark conclusions that emerge from the above analysis are:

- Indian media does not have a wider perspective of India's national security issues.
- Indian media is in no mood to apply brakes or observe self-restraint on its wayward and insensitive treatment of national security issues.
- Indian media's (especially electronic media) analysis and over-analysis of national security issues by groups of former diplomats, generals and academia's arm chair strategists distort national security perspectives. All these gentlemen can only draw on their outdated experience and none of them are privy to latest inputs. Also in many cases, reticence is their first casualty after retirement.
- Indian TV anchors discussing national security issues do not have the political and strategic maturity to discuss national security issues as their Western counter-parts do.
- Indian TV debates on national security issues tend to cut out development of contrary views and perspectives by imposing commercial breaks, or go hectoring themselves.

National security of India is paramount and the Indian media under the guise of 'press freedom' cannot claim unfettered sway and freedom for non-objective means. The Government and the media need to sit down together and come out with a system of guidelines, self-restraints and other forms of moderation to ensure that the media does not distort or 'jeopardise' India's national security interests. In case the media is not receptive to self-restraint, the government would be well within its rights to come up with stringent measures.

India's survival as a nation-state is at stake due to both external and internal threats. The armed forces, the para-military forces, and the police are staking and losing their lives to defend the country against such threats. Indian governments of any political hue should not permit trivialising or jeopardising India's national security issues by the media.
The Indian media needs to appreciate that while idealism and extreme forms of liberalism may be permitted in political coverage and analysis, these cannot be applied to national security issues. Also, over-analysis and sensationalism may be their bread and butter in the political field, but it cannot be permitted in national security issues.

## Quashing Dissent: Where National Security and Commercial Media Converge

Between February 14 and 15 of 2013 , the Department of Telecommunications (DoT) in the Government of India issued five separate orders to internet service providers (ISPs), blocking access to no fewer than 164 URLs or web addresses where specific content is hosted. All five were issued in seemingly unquestioning and unreserved compliance with *ex parte* orders emanating from courts. No reasons were given, though as things transpired, these were not very difficult to figure out. Of the

five orders, three were issued with clear intent to clamp down on protests in Kashmir after the February 9 execution of one-time militant Mohammad Afzal Guru. Physical movement in all of Kashmir had been blocked by a pre-emptive curfew imposed early that morning. As news of the execution filtered through, local news channels and newspapers were told to suspend operations. And though the internet remained available through broadband, the more widely used modes of access in the valley -- mobile telephones and wireless data cards – were disabled. The information lockdown persisted five days in the case of newspapers and an entire week for internet users. For local TV news channels, it still continues. But through the pores in this blanket of censorship, the people of Kashmir were still managing to make their anger and bitterness heard. The DoT directive, calling specifically for the shutting down of a number of pages on the social networking site "Facebook" was obviously about shutting that source of dissent. An information blockade imposed on a region where rights to life and liberty have been in suspension might seem a lesser injustice, though it is part of the same apparatus of repression that particularly targets any possibility that an occupied people may conduct a social dialogue that reaches beyond immediate constraints of location and space. Yet for all that, there was nothing really unusual about the effort to tighten the information blockade on Kashmir, a region that has long been in a state of exception in the Indian political map, where even the pretence of guaranteed rights and entitlements does not apply. Indeed, a similar blockade on mobile telephone services had been imposed in the valley just a fortnight prior, while the rest of India was celebrating the anniversary of its republican constitution.

A second category of website blocks ordered in DoT's most recent round of sweeping censorship, applied against the mimicking or parodying of important public institutions, such as the Bombay High Court. Few dissenting voices were raised here. If anything, there may have been some reservations about the recourse to heavy-handed censorship, where the task of sifting between the authentic and the fake, might well have been left to the judgment of the internet user, worries that the DoT action may have cast the rare visitor to these sites as an infant in need of the guiding hand of a nanny state.

## The IIPM related blocks

What really raised eyebrows and triggered a war of attrition on the internet was the third category of order issued by the DoT, blocking seventy-three specific web addresses ranging over a total of fifty websites. The formal order addressed to all ISPs, began with a peremptory, "it has been decided", much like an edict issued from a sovereign that is beyond challenge. After listing the sites to be censored, it entered a plea for secrecy, uncharacteristic for a sovereign acting with absolute authority. Letters of compliance to be filed by all those at the receiving end of the edict were not to mention the identity of the blocked URLs.

If the intent of that caution was to conceal the identity of the guiding hand behind this extraordinary measure of information denial, it did not go far. The common element in the seventy-three web addresses that were blocked was soon discovered to be the Indian Institute of Planning and Management (IIPM), an establishment with a pervasive presence in the media, despite its uncertain provenance and rather anomalous status within the landscape of higher education, where it claims to belong. Indeed, the IIPM advertising budget, the envy of most other institutions in the same category, wins it a high degree of exemption from scrutiny in the mainstream media. No such privilege though, is granted within the alternate discourse of the social media. Indeed, that is where the problem was clearly seen to lie.

Cryptic in its content and opaque in terms of its legal basis, the DoT order was traced by the small but vigorous community of free speech advocates on the internet, to emanate from an order by a court in the city of Gwalior in Madhya Pradesh. For the most part, it applied to blogs and independent initiatives by consumer groups and civil society actors to promote a dialogue on issues of public concern: such as the quality of service offered by various civic and commercial institutions. The IIPM, unsurprisingly for an institution with a high media profile, had come in for some searching scrutiny and been found wanting: several of the postings on these sites, drawing on first-hand experiences of the services (or lack of it) that it offered, were trenchant in tone and content.

It emerged soon afterwards that the Gwalior court had issued its order under provisions of the Indian Penal Code (IPC, section 499) dealing with the offence of defamation and the Information Technology Act (IT Act, section 69) which enabled government authorities to demand the blocking of certain sites by ISPs and intermediaries such as Google and Facebook. Evidence that the court had applied the tests of intent, accuracy and public interest that are the preliminaries mandated by law before sanctions are imposed for defamation, was conspicuously lacking. And what literally leapt out in the DoT edict was the very first URL on the list, which belonged to a public institution, the University Grants Commission (UGC). In a notice issued in July 2012, ostensibly in compliance with a directive issued by the Delhi High Court in ongoing litigation, the UGC had recorded its finding that the IIPM was not a university under applicable law. It was in other words, not empowered to grant degrees in business management or any other discipline of study.

In holding the UGC liable for defamation, the Gwalior court obviously omitted any serious engagement, either with the history of litigation involving the IIPM, or with the law. Section 499 of the IPC is explicit about certain exceptions where in circumstances to be judged by the courts, the offence of defamation would not apply: these include, the "imputation of truth which public good requires to be made or mentioned," the "public conduct of public servants" and the "conduct of any person touching any public question". Clearly, any assessment that the UGC may have made about the academic credentials of the IIPM, when communicated to the public, would potentially fall within the scope of these exceptions. That the Gwalior court overlooked these aspects of the law points towards an egregious omission.

## "Hacktivist" Response

Internet activists were quick to wreak vengeance. On Friday 16, the website of the IIPM was hacked and put out of service for a limited period of time. And under pressure from a growing chorus of outrage, the owner and executive head of the institution, Arindam Chaudhuri, took to the social network to explain his actions. The court order applied only to website content that was defamatory in an explicit sense, he pleaded. Satirical sites may have been included in an over-broad sweep of content pertaining to the IIPM, but remedies would be quickly instituted once a closer examination was made. As for the UGC and one other public institution in the education sector – the All India Council for Technical Education (AICTE) – Chaudhuri was scathing in his assessment: "I should say UGC and AICTE are organisations full of bribe-seeking corrupt officials where, even at the top, they have a track record of being caught red-handed and being jailed. I suspect that UGC – at the behest of some of our petty competitors with dirty past records of filth and cheating, and public notices against them – had been deliberately spreading misleading information about IIPM to hurt its business interests and had even gone to the extent of falsely calling IIPM a fake university".

There is much that is specious in the IIPM explanation and a great deal that the judiciary has to explain about its manifestly perverse order. Within days of the DoT implementing its blocking order, the Department of Information Technology (DIT) – a partner department under the Ministry of Communications – resolved on appealing it at the appropriate judicial forum. That may well have been too little too late. As the senior advocate and legal scholar Rajeev Dhavan has pointed out, in all such matters "the real mischief takes place right at the beginning … when injunctions are freely granted to prevent the publication or dissemination of an existing or proposed publication".

The IIPM is a practised hand in censorship through legal injunction. In June 2011, it filed suit against *Caravan*, a monthly magazine of political and cultural commentary, for the sum of Rs 50 crore (INR 500 million), after the magazine had in its February 2011 issue, featured an article titled "Sweet Smell of Success: How Arindam Chaudhuri Made a Fortune Off the Aspirations — and Insecurities — of India's Middle Classes". The article was a substantive pre-publication excerpt from a book by U.S.-based journalist Siddhartha Deb, due for publication in July 2011. The IIPM lawsuit named the author, the publisher Penguin Books (India) and the internet search portal Google (India) as respondents, other than *Caravan*, accusing them of "grave harassment and injury". The lawsuit was filed not in Delhi, where both the IIPM and *Caravan* are based, but in Silchar town in the north-eastern state of Assam. IIPM was the second petitioner, the first being a Silchar businessman known to be associated with the institute as a recruiter. At the first hearing of the case, the civil court in Silchar granted the IIPM a preliminary injunction, enjoining *Caravan* to remove the impugned article from its website. This decree was issued *ex parte*, without any pre-hearing notice to the magazine. The article was since taken off the *Caravan* magazine website, though it has been retained in the Internet Archive. In the most recent round of court-ordained censorship, the magazine's July 2011 announcement that it intended to fight the injunction was blocked, but then republished under a different URL.

In October 1972, India's Supreme Court heard a case brought by Bennett Coleman and Company Ltd (BCCL), publishers of the *Times of India* – and a number of other large newspaper enterprises – challenging a newsprint rationing order introduced to deal with a situation of acute scarcity. The official plea entered on behalf of the rationing was that the larger newspaper groups would, if allowed unfettered access to the market, buy up all the supplies available, depriving smaller players – and with this, large sections of the Indian population – of the means to speak and be informed. The judgment in the case of Bennett Coleman and Co Ltd v Union of India is one of historic significance, since it remains the most authoritative statement yet, on how the constitutional guarantees of free speech devolve into the narrower construct of media freedom. Yet this is a judgment that remains strangely inconclusive, since in addressing the issue of the free speech right, the majority opinion of the Court seemed to oscillate rather indecisively, between a notion of free speech as a privilege enjoyed by the few, and a broader conception of the unreserved exercise of the right by all.

In deciding the case, Justice A.N. Ray spoke for the majority and observed that the "individual rights of freedom of speech and expression of editors, directors and shareholders, are all expressed through their newspapers". But then a few pages on, the majority opinion effectively widened the ambit of the right: "It is indisputable that by freedom of the press is meant the right of all citizens to speak, publish and express their views. The freedom of the press embodies the right of the people to read. The freedom of the press is not antithetical to the right of the people to speak and express".

Having elevated media freedom to a higher plane and rendered it into an entitlement enjoyed by all citizens, the majority in the *Bennett Coleman* case had little difficulty striking down newsprint rationing as a violation of article 19 guarantees on free speech. The rest of the majority judgment in the matter clung very closely to the liberal orthodoxy on the right to free speech: that governmental regulation is an evil more invidious than private monopolies. When it looked at the prospect of "monopolistic combination" in the press, it was only to rule it out. And even if the likelihood did arise, newsprint allocation could not be a feasible "measure to combat monopolies".

Of special significance in this context is the lone dissenting judgment delivered from a bench of five judges, by Justice K.K. Mathew, who explicitly conceded the possibility of a conflict between the public interest and the profit motivations of the press. Using a "theory of the freedom of speech" that essentially viewed it in terms of twin entitlements -- to speak and be informed – Justice Mathew observed that "the distribution of newsprint for maintenance of (newspaper) circulation at its highest possible level (Would). Only advance and enrich that freedom". As a constitutional principle, "freedom of the press" was "no higher than the freedom of speech of a citizen". The problem at hand was one of bringing "all ideas into the market (to) make the freedom of speech a live one having its roots in reality". In pursuit of this ideal, it was necessary as a first step, to recognise "that the right of expression is somewhat thin if it can be exercised only on the sufferance of the managers of the leading newspapers".

Freedom of expression in other words, also involved the right of access to media space. And this requirement would be met only through the "creation of new opportunities for expression or greater opportunities to small and medium dailies to reach a position of equality with the big ones". This was as important, in Justice Mathew's judgment, "as the right to express ideas without fear of governmental restraint". What was required was an interpretation of the free speech right which recognised that "restraining the hand of the government is quite useless in assuring free speech, if a restraint on access is effectively secured by private groups".

## Indian Media – An Echo Chamber for the elite

For all the appearances of growth and diversification that it presents, there is increasing worry that the Indian media with its advertisement-driven revenue model is becoming an echo chamber where those with economic clout and purchasing power talk among themselves, leaving out the voices of the vast majority. Citizens who happen to inhabit the zones of exception, such as Kashmir and he north-east, are excluded from participation by virtue of their infirm commitment to what is by elite consensus, deemed the "mainstream" ethos of Indian nationalism. And the socially and economically disadvantaged in other parts, are inconsequential because they are of no interest to the advertiser who sustains the media industry bottom-line. In this context, the growing number of social media users offers a potent challenge to the hegemonic narrative that emanates from the mainstream media. The most articulate voices here emerge from the top two or three percentiles of the population, who have access to the estimated 14 million broadband internet connections. But within this narrow stratum, there is already more dissent against the news priorities and editorial policies of the mainstream media, which in terms of reach addresses a multiple – though not a very large multiple – of broadband users.

More worrying for those who believe media freedom is a great idea as long as a few wise men control the message, is the rapid growth of internet and social media users through the mobile phone

network. This is a growing constituency in Kashmir, the north-east and indeed, in several regions of the most bitter political contestation in India: territories where the promise of the minority judgment in the *Bennett Coleman* case is actually being sought, that media freedom is not just a right to be exercised on "sufferance" of those who own newspapers or the airwaves, but a right that all citizens have to speak and be heard, even beyond limitations of location and space.

There is a long history of repression of this manner of free speech, but few instances where sanctions have been imposed on speech that meets every authentic criterion of "hate". This is unsurprising, since this category of speech usually emanates in the Indian context, from Hindutva and other such supposedly "mainstream" participants in the national consensus. The February crackdown on websites is probably just a minor punctuation mark in the long-term evolution of the doctrine of "legitimate" repression of basic rights, when exceptions to the rule of free speech could be decreed. It is nonetheless, a point at which some clarity is imparted. Constitutional guarantees seem a distant, almost illusory promise when the politics of the street -- and a loud and seriously misinformed media – are final arbiters of fundamental rights and the defence of privilege is becoming the dominant motif of state policy. This most recent information blockade targets political dissent from the fringes of "mainstream" nationalism and also a prospective challenge to the commercial calculus of the "mainstream" media. It shows how close the convergence is, between the propaganda needs of the national security state and the commercial compulsions of the mainstream media. Finally though, what is most apparent about this new effort at controlling the message is its utter futility, since the avenues through which people can speak and be heard are multiplying in such diverse ways, that information repression no longer is an option for states anxious to preserve control.