APC IMPACT
India . Malaysia . Pakistan
Advocacy for Change Through Technology

internet RIGHTS

DEF
DIGITAL EMPOWERMENT foundation

Limited Access Restricting Expression

COUNTRY RESEARCH REPORT

DIGITAL EMPOWERMENT FOUNDATION

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Background to the report

- First year outcome under the Advocacy for Change through Technology in India, Pakistan and Malaysia (IMPACT) Project of the Association of Progressive Communications (APC) under the Internet Rights project at DEF
- Supported by the European Union under the European Instrument for Democracy and Human Rights
- Based on the APC-Frank La Rue (FLR) Framework; adapted from the work of Frank La Rue, Former UN Special Rapporteur on Freedom of Opinion & Expression
- Other Activities under the IMPACT Project:
  - Trainings with academia and grassroots beneficiaries on Internet Rights in India
  - Organising multi-stakeholder international workshops at Internet Governance Forum (IGF), RightsCon etc.
  - Engagement on and submission of position papers on WSIS, Net Neutrality and others.

Digital Empowerment Foundation

DIGITAL EMPOWERMENT *foundation*
empowering people @ the edge of information

A non-profit organisation dedicated to find sustainale Information Communication Technology (ICT) solutions including digital & new media to address digital divide in under-served and unreached regions and communities.

- Access & Infrastructure – CIRC, Wireless for Communities, MCGY
- Education & Empowerment – NDLM, District Public Libraries Programme
- Governance – Soochna Seva
- Social Sector & CSOs – e-NGO, Neerjaal, e-Heritage
- Markets & Enterprise – Chanderiyaan, DigiKala
- Knowledge Network – Manthan Award, m-Billionth Award, e-NGO Award, Social Media for Empowerment Award
- Research & Advocacy – Internet Rights, Mobiles for Social & Behavioural Change

Introduction to the report

Human rights in India are guaranteed under:

- Constitution of India
- Universal Declaration of Human Rights
- International Covenant on Civil & Political Rights

Indicators under FLR Framework

- General Protection of Freedom of Expression
- Arbitrary Blocking or Filtering
- Criminalising Legitimate Expression
- Imposition of Internet Intermediary Liability
- Disconnecting Users from the internet
- Cyber-Attacks
- Protection of the Right to Privacy and Data Protection
- Access

Methodology of the Report

Adapting the APC-FLR Framework to Indian context - to guide research, evidence collection and mapping of laws & policies

Review of existing legislations & case law - to draw trends and understand practices in India

Stakeholder consultations & interviews

Quantitative survey across India (10 states, 600 respondents) - to understand the ground level realities viz. the FLR Framework

- Ownership, Use Profile, Accessbility & Application
- Status of Rights and
- Gauge the level of understanding

Indicators of the FLR Framework

Indicator 1 - Access

Overall internet penetration is very low – lowest in rural areas

Sub-indicator 1 - State has a national plan of action for internet access

Digital India plans to integrate the National Optical Fibre Network (NOFN), Government User Network (GUN), State Wide Area Network (SWAN), NICNET and National Knowledge Network (NKN) into a comprehensive network backbone.

- NOFN is still a work in progress
- DEF conducted a review of the 59 pilot blocks
  - 45.5% of the 112 institutions had a working NOFN connection
  - 21.4% have a hard line connection but no access to the NOFN
  - 20.5% have no connection to the NOFN

Delhi Metro is deploying wifi connectivity in Central Delhi stations on the network

Indicator 1 - Access

Sub-indicator 2 – State fosters independence of new media

Trends show that use of social media will increase in India

Government institutions have also started using social media to connect

- Framework & Guidelines for Use of Social Media for Government Institutions has been created by DeitY

Additional Solicitor General of India (during the Shreya Singhal Case) argued that social media is a form of media that has a much greater reach and potential influence than traditional media.

Each individual is a publisher, printer, producer, director and broadcaster of content without any regulatory oversight.

Indicator 1 - Access

Sub-indicator 3 - Concrete and effective policy is developed with public and private sector to make the internet available, accessible and affordable to all

Google & Microsoft to deploy connectivity services and/or training centres in India

Significant conversations surrounding the Net Neutrality argument in India has occurred

- 1.09 Lakh responses to TRAI OTT consultation paper from Service Providers, Service Providers' Associations and Other Stakeholders (individuals, organisations & consulting firms)

DOT Committee Report has submitted its recommendation to TRAI, however, they are still to be adopted – Shows promise as well as cause for concern

- Licensing for domestic VoIP
- Zero rating to be allowed on case by case basis by TRAI

Indicator 1 - Access

Sub-indicator 4 - Development programmes and assistance policies facilitate universal internet access

Out of the 9 pillars of the Digital India Plan, 4 deal with universal access

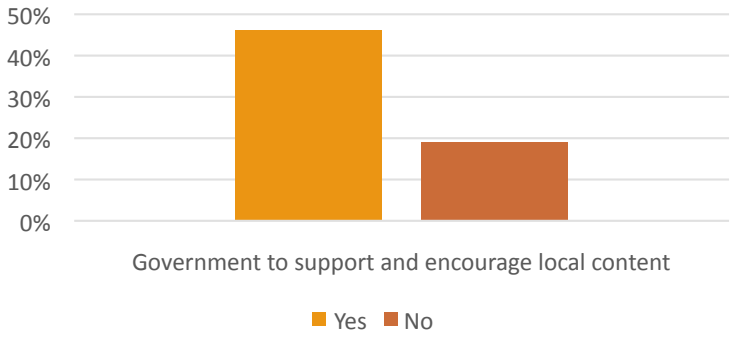
- Broadband Highways
- Universal Access to Mobile Connections
- Public Internet Access Programme
- Information for All

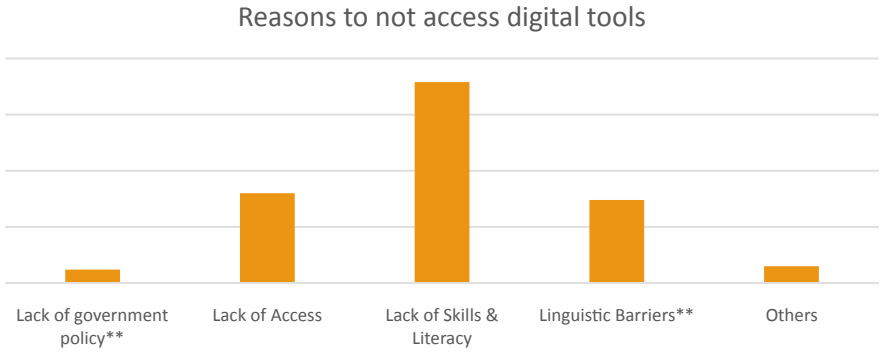
Indicator 1 - Access

Sub-indicator 5 - State supports production of local multicultural and multilingual content

DEF primary study shows that 46% of the population wants the government to support and encourage local content

In another, newer DEF study, out of 360 respondents, 74 stated that they do no access digital tools due to the unavailability of any resource in their language





Indicator 1 - Access

Sub-indicator 7 - Digital literacy programmes exist, and they are easily accessible, including primary school education and training

National Digital Literacy Mission - make 1 person from each household digitally literate by 2019.

Challenges to Access

- Infrastructural issues are a key barrier to access - non-functioning computers and poor roads —> digital and external (physical) connectivity are important factors
- Connection Vs. Connectivity - Infrastructure - Power, internet access, roads, toilets
- Affordability - Respondents stated that it is easier for them to travel to access the internet due to high personal internet connectivity costs
- Digital Literacy - Need for trained, quality technical professionals with basic computer and digital literacy
- Socio-cultural and political norms
  - 60% of respondents stated that family, children and community obligations prevent them from accessing the internet
  - 23% of women stated that their family does not allow them to access the internet as it might make them a 'bad person'.

Indicator 2 – Disconnecting Users from the Internet

Sub-indicator 1 - Internet access is maintained at all times, including, during political unrest

There have been many instances where internet access has been blocked for individuals in an affected region

- July 2013 - Internet access was blocked in Jammu & Kashmir
- February 2014 - Jammu & Kashmir access was blocked again
- March 2015 - Internet & SMS services in Nagaland were blocked after a video of the lynching of a rape accused went viral.

During the protests by the Bajrang Dal against the PK movie, internet access was maintained. BJP President Amit Shah made a statement regarding ensuring Freedom of Expression; even against PK.

Indicator 3 – Imposition of Intermediary Liability

Section 79A and Intermediary Guidelines, 2011 allows the government to order intermediaries to remove/block/modify content that it deemed objectionable. The term "objectionable" was also subject to the classification in Section 66A. Police could give an order to remove content.

In 2013, the government clarified the process for takedown of any objectionable material

- Before 2013 → Intermediaries has 36 hours to follow an order
- After 2013 → 36 hours to acknowledge & 1 month to comply. Failure to comply was subject to litigation.

in 2015, the Shreya Singhal case, generated widespread change in the overall field of intermediary liabilities.

- Section 66A was struck from law; the vague definition of "objectionable" was removed along with it.
- Section 79A was "read down"; Intermediaries can act only on a court order or a notice from the government or its agency.
- Intermediaries are not liable for user-generated content and do not have to undertake self-policing

Indicator 3 – Imposition of Intermediary Liability

Sub-indicator 1 - State does not delegate censorship to private entities

The Government does not have a formal policy in place; however, has been placing pressure on private entities.

- MouthShut.com Vs. Union of India : Intermediaries are not needed to conduct self-policing. Lack of technical expertise, manpower and time inherent with intermediaries has been recognised
- PUCL vs. Union of India : Private entities are allowed to adjudicate over content without legislative guidance and without informing the party affected by the censorship. Offline & Online content should be treated the same.

Indicator 3 – Imposition of Intermediary Liability

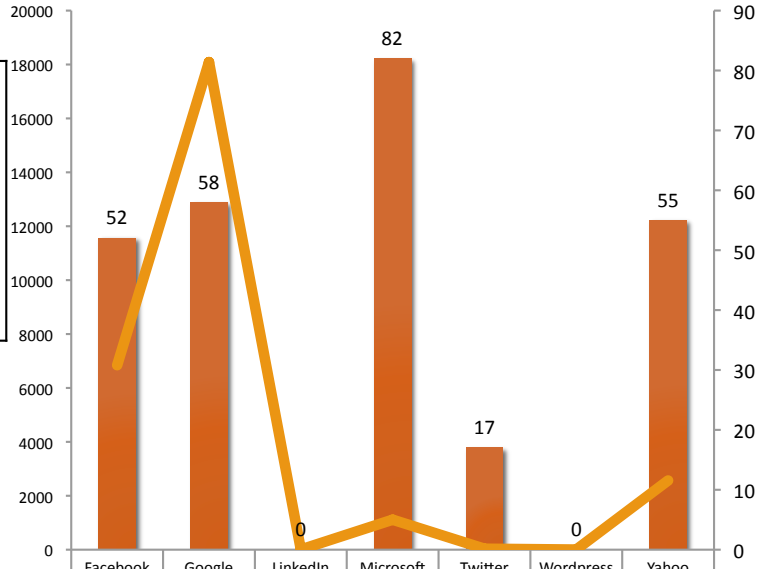
Sub-indicator 2 - State's requests to internet to prevent access to content or are disclose private information are 1) strictly limited to purposes such as administration of criminal justice and 2) by order of a court of independent body

Compliance rates differ across different intermediaries.

- Twitter: 7%
- Google: 61%

State's requests are not limited to criminal justice only —> Removal of blog post about a politicians' sex scandal. Google did not comply with this request.

NOTE - Time periods for company data
* Facebook (2013)
*Microsoft (2012 to 2013)
*Wordpress (2013 2nd Half)
*Google (2009 (2nd Half) to 2013)
*Yahoo (2013)
*LinkedIn (2011 (2nd Half) to 2013 (2nd Half)
*Twitter (2012 - 13)



	Facebook	Google	LinkedIn	Microsoft	Twitter	Wordpress	Yahoo
Compliance Rate (Percentage)	52	58	0	82	17	0	55
Total Requests	6843	18090	6	1112	35.5	5	2568

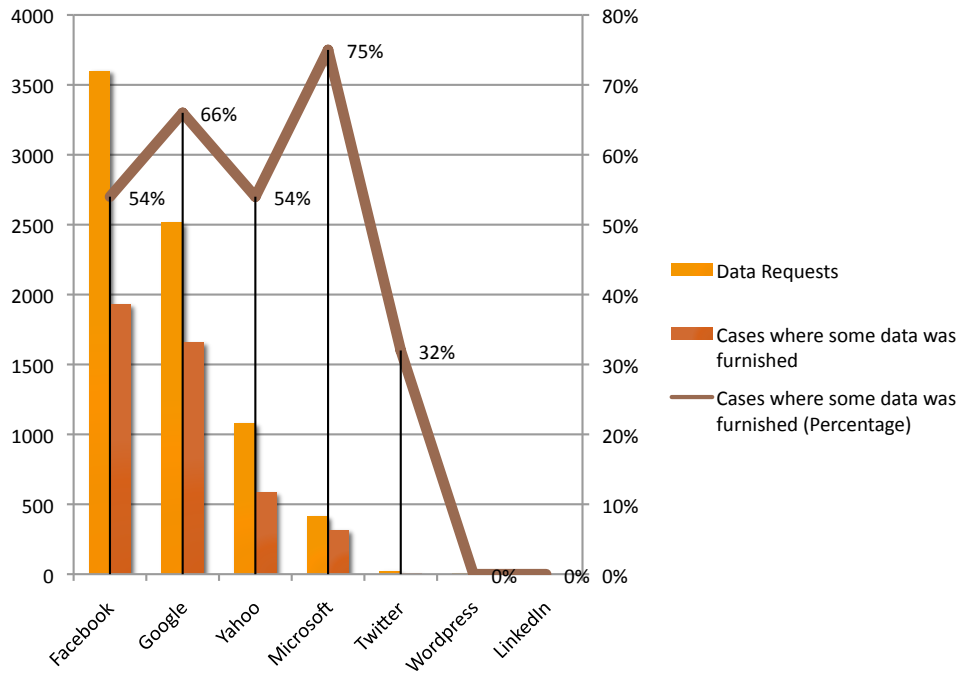
Indicator 3 – Imposition of Intermediary Liability

Sub-indicator 3 - State discloses details of content removal requests and accessibility of websites

The Government does not always disclose the details of removal requests. It has done so at times. However, most of the time, it asks intermediaries to remove such content.

Major intermediaries publish transparency reports that highlight some of the details regarding these removal requests.

Civil society groups argue that the the lack of transparency from the government's end is a major issues. Additionally, there is a tendency to misuse national security & religious sentiments for blocking



Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 1 - There are no generic bans on content

Laws prohibit the distribution & sale of porn. However, viewing pornographic content is not a crime under the law

Section 69A of the IT Act allows blocking of websites

IMPACT meeting stakeholders questioned the definition of “generic bans” in India

Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 2 - Sites are not prohibited solely because of political or government criticism

Government does not need to provide an explanation for banning any content

Political or government criticism is not always shut down. However, there are some exceptions:

- AAP Activist from Karnataka was arrested for circulating MMS with Modi's likeness on a corpse with the slogan "Abki Baar Antim Sanskaar", which spoofed the BJP campaign slogan
- India's Daughter was banned from being broadcasted in India. The government cited the "encouragement & incitement of violence against women" as the main cause

Conversely, a Change.Org petition for the Government to stop using Yoga Day to enforce cultural homogeneity has been left by the wayside and been ignored.

Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 3 - State blocks or filters websites based on lawful criteria

Content blocking falls under the ambits of Article 19(2) of the Constitution, Section 69A of the IT Act and The Information Technology (Intermediaries Guidelines) Rules, 2011.

In December 2014, 32 websites we blocked with the government stating that they contain “objectionable content”. The term “objectionable” is too vague

There have been multiple instances where websites have been blocked under similar vague circumstances

Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 4 – State provides lists of blocked and filtered websites

The Government does not provide the list of blocked websites always; instead on a case-by-case basis.

Department of Telecommunication issues the notification for public consumption. In the case of the 32 websites that were blocked, after a screenshot of the list was leaked, the Head of the IT Cell of the BJP tweeted that they were blocked because they carried anti-India content.

The IT cell of the political party provided an explanation before the Government!!

Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 5 - Blocked or filtered websites have an explanation on why they are blocked or filtered

In the list of 32 websites mentioned earlier, Github and Pastebin; two valuable resources for programmers in India, were blocked.

Administrators of both websites posted that they did not have prior information about the blocking and were trying to reach out to the Indian Government to sort the issue out.

We request government to be more transparent with its review process; committee member details and the outcomes.

Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 6 - Content blocking occurs only when ordered by competent judicial authority or independent body

There is a review process to blocking access to content.

A Designated Officer nominated by the Central Government chairs a committee that has members that represent the ministries of Law, Home Affairs and Information Technology along with members from Computer Emergency Response Team (CERT).

In case of an emergency, the Designated Officer and Secretary, DeitY can issue blocking orders. However, the content will have to be unblocked in case the committee does not give its approval to the block.

The DO is supposed to follow court orders after submitting the order to the Secretary, DietY

Indicator 4 – Arbitary Blocking & Filtering

Sub-indicator 7 - Where blocked or filtered content is child pornography; blocking or filtering online content is connected with offline national law enforcement strategies focused on those responsible for the production & distribution of content

Section 67B of the IT Act deals with the browsing, downloading, creation, publication and distribution of child pornography.

Child sexual abuse laws have been included in the National Child Protection Policies.

It is unclear as of yet if blocking or filtering of online child pornography is connected with offline law enforcement strategies.

Indicator 5 – Protection of the Right to Privacy & Data Protection

SUB-INDICATOR 1 - THERE ARE ADEQUATE DATA AND PRIVACY PROTECTION LAWS AND THEIR APPLY TO THE INTERNET

There have been two draft Right to Privacy bills tabled; one in 2011 and one in 2014

- 2011 Version: To cover all state & non-state actors that collect data and to ensure that this information was not misused. Extended the Right to Privacy to all **citizens** of India.
- 2014 Version: It extended the Right to Privacy to all Indian **residents** (incl. Jammu & Kashmir). However, the bill included exceptions to data collection by insurance & government intelligence agencies "*in the interest of national sovereignty, integrity and security or strategic, scientific or economic interests of the country*"

The Central Monitoring System (CMS) has been created by C-DOT under the ambit of the Telecom Enforcement Resource and Monitoring team.

The Government has set up the Data Protection Authority to look into issues surrounding privacy.

Indicator 5 – Protection of the Right to Privacy & Data Protection

SUB-INDICATOR 2 - STATE DOES NOT REGULARLY TRACK THE ONLINE ACTIVITIES OF HUMAN RIGHTS DEFENDERS, ACTIVISTS AND OPPOSITION MEMBERS

The rollout of the CMS, a mass surveillance system by C-DOT raises concerns regarding the protection of Human rights defenders, activists and opposition members.

Facebook accounts of activists are suspended

Judiciary is not always educated w.r.t. ICT tools and the online implications of Human Rights

Indicator 5 – Protection of the Right to Privacy & Data Protection

SUB-INDICATOR 3 - STATE DOES NOT ADOPT A REAL NAME REGISTRATION POLICY

India adopts and enforces a real name registration policy

- UIDAI
- Cellphone connections
- Cyber cafes
- New email accounts need to be verified by One-Time-Password (OTP)

Indicator 6 – General Protection of Freedom of Expression

SUB-INDICATOR 1 - NATIONAL CONSTITUTION OR LAWS PROTECT INTERNET BASED FREEDOM OF EXPRESSION

Article 19(1)(a) of the Constitution protects freedom of speech & expression. Article 19(1) encompasses a wide range of protections; expression, speech, association, assembly, residence and occupation & trade

- However, Article 19(2) places "reasonable restrictions" on the protections under Article 19(1)

Indian Penal Code, 1860

- Section 124A - Punishes sedition
- Section 153 - Penalises offences that promote animosity between groups on the grounds of religion, race, place of birth etc.
- Section 295A - Punishes acts that are deliberate & malicious and that aim to outrage religious sentiment
- Section 500 - Punishes defamation

Indian Telegraph Act, 1885

- Section 5 - Interception of messages
- Section 9 - Creation of the Universal Service Obligation Fund (USOF) to ensure access

Indicator 6 – General Protection of Freedom of Expression

Information Technology (IT) Act, 2000 and the amendments of 2008 create powers of the government that extend to the online space:

- Section 66A - Makes punishable communications that are deemed "offensive", false or causes annoyance. - Shadowed by Supreme Court for being "unconstitutional"
- Section 66E - Makes punishable capturing any image of the private areas of an individual that infringes on privacy
- Section 66F - Punishes acts of cyber-terrorism
- Section 67A - Punishes creation and transmission of sexually explicit content
- Section 67B - Punishes publication or transmission of any sexually explicit material that involves minors.
- Section 69 - Powers to intercept & monitor communications
- Section 69A - Powers to order intermediaries to block content (Intermediary liability)
- Section 69B - Powers to monitor communications for cyber-security
- Section 79 - Exemptions to intermediary liability and links to Intermediary Guidelines

Indicator 6 – General Protection of Freedom of Expression

SUB-INDICATOR 2 - STATE PARTICIPATES IN MULTI-STAKEHOLDER INITIATIVES TO PROTECT HUMAN RIGHTS ONLINE

Participates in the Universal Periodic Review (UPR) of the Human Rights Council.

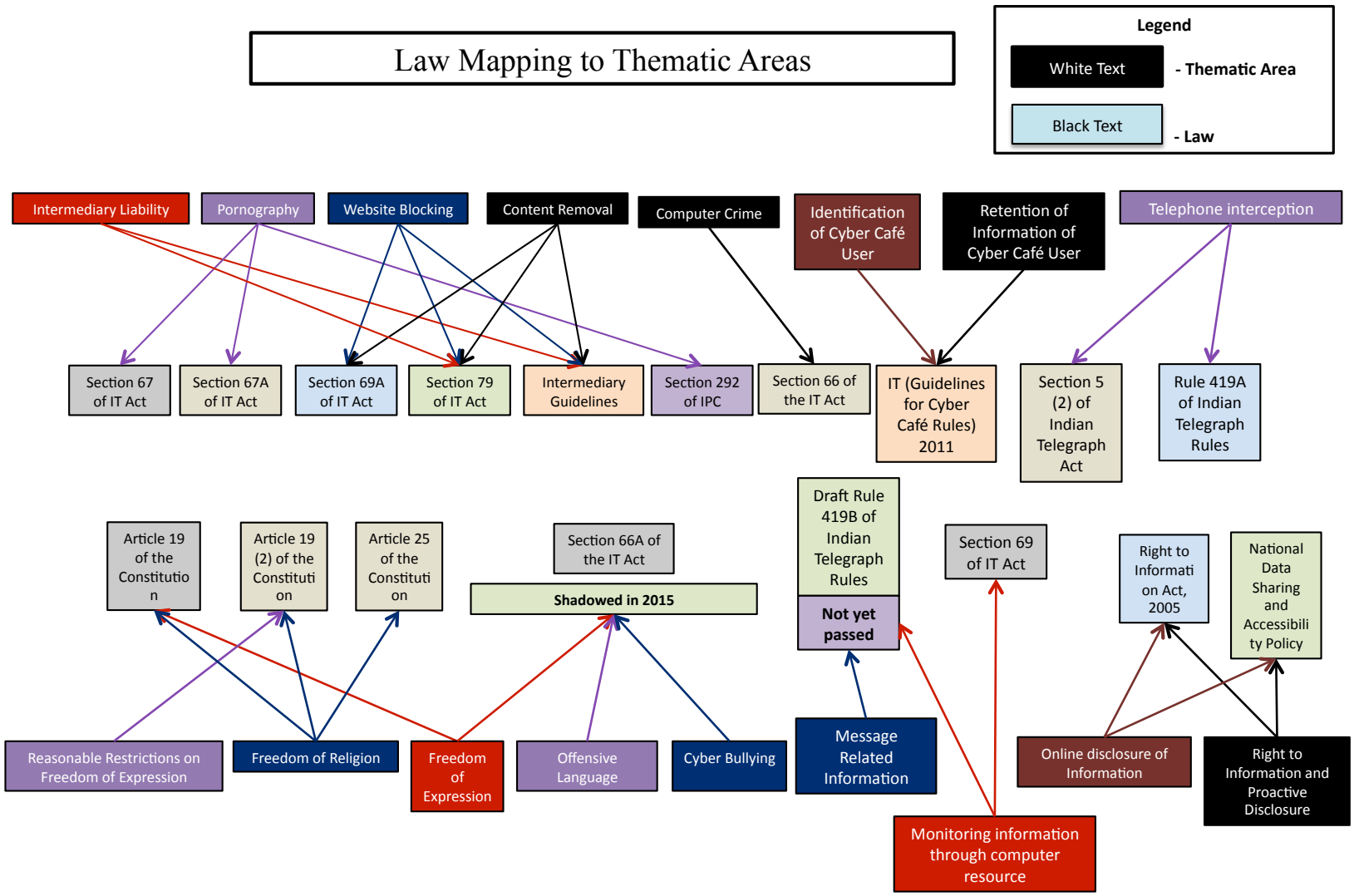
- In the second UPR cycle, India recognised the importance of Right to Information & Right to Education. However, India **did not adopt** the recommendations towards online freedom of expression & opinion.

In-country multi-stakeholder initiatives are opaque; few organisations are invited, place & time are often unknown and outcomes are not known.

A small set well-funded & prominent CSOs have access to these consultations.

India has shifted between promoting multi-stakeholder approaches to government-led approaches in different fora.

Law Mapping to Thematic Areas



Kumar, R. (2015)

Indicator 7 - Criminalising Legitimate Expression

SUB-INDICATOR 1 - JOURNALISTS & BLOGGERS ARE PROTECTED AGAINST ABUSE OR INTIMIDATION

The Press Council of India has a clear definition of the “Journalist”. However, “Blogger” is not very well defined by the PCI.

In January 2015, The National Crime Records Bureau reported 85 attacks on the media in 2014, 10 threat cases and 3 cases of harassment.

Tushar Sarathy and Jaison Cooper were arrested under the Unlawful Activities Prevention Act (UAPA) in Kerala after their blog posts shed light on a number of struggles by marginalised and dispossessed people in India.

Section 15(2) of the Press Council Act provides protection to the “Journalist” from revealing his/her sources. This protection is not extended to the “Blogger” and is not applicable to the “Journalist” in court.

Journalists also face harassment within their own organisation.

Indicator 7 - Criminalising Legitimate Expression

There exists a triangular relationship between Media Institutions, Political Parties and Economic Interests. Conflicts of interests spill over and compromise journalistic integrity.

Not many news organisations support their journalists in the face of abuse and harassment.

Transfer of Doordarshan Assistant Director V.M. Vanol from Gujarat to the Andaman Islands for airing a story about Mrs. Modi filing an RTI about her security arrangements.

Pankaj Shrivastava, Associate Director of IBN7 was fired for raising an issue of non-coverage of Aam Aadmi Party win in Delhi state. He is now following up with legal action against the channel.

It has become hard to cover some topics, leading journalists to forget journalistic ethics in favour of protecting their job.

Indicator 8 – Cyber Attacks

The Data Security Council of India defines

- Cyber Crime as "*deliberate actions to alter, disrupt, deceive or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks*".
- Cyber Attacks as "*Crime where the computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, hate crimes etc.)*".

The two terms are used interchangeably.

Indicator 8 – Cyber Attacks

SUB-INDICATOR 1 - STATES TAKES APPROPRIATE AND EFFECTIVE MEASURES TO INVESTIGATE ACTIONS BY THIRD PARTIES, HOLDS RESPONSIBLE PERSONS TO ACCOUNT AND ADOPTS MEASURES TO PREVENT RECURRENCE

The government has been taking **reactive** and **proactive** measure to combat cyber crime and cyber attacks.

Reactive Measures

- Creation of the Cyber Emergency Response Team (CERT) to serve as the national agency for:
  - information on cyber incidents, forecast & alters on cyber incidents, emergency measures, coordination of response activities, issuance of guidelines, advisories and white papers
- Proposed creation of National Cyber Coordination Centre
- The DSCI and CBI have signed a MoU to strengthen the abilities of law enforcement

Proactive Measures

- Draft National Cyber Security Policy (NCSP)

However, NCSP is duplicating efforts of the CERT instead of building on it.

Recommendations

Government should be transparent in terms of blocking, filtering and removal of the content and comply with international standards.

The CMS and UID systems be reviewed and reformed so that it is in line with international standards regarding the right to privacy.

The government, in collaboration with all stakeholders expand quality internet access in a transparent, accountable, and affordable manner so that communities can access quality and timely public services—and become aware of and begin exercising internet rights as part of basic human rights in the 21st century. In this context, opportunities are increasing to advance development and human rights, particularly FoE and FoAA which can enable good governance and strengthen democracy.

National Commission on Human Rights incorporate internet rights as part of their approach to human rights, as articulated by the UN Human Rights Council. This step would raise awareness about internet rights in both urban and rural India.

Recommendations

It is recommended that civil society organisations collaborate with private sector, government, industry bodies and educational institutions to raise awareness about internet rights, within the human rights framework, particularly FoE and FoAA among grassroots citizens.

It is further recommended that all stakeholders incorporate the following components within:

- Understand the importance and purpose of access and ICT tools
- Deconstruct internet rights and human rights
- Understanding the concepts of FoE online and international and national legal mechanisms
- Encourage understanding of responsible digital citizenship and
- Security

Recommendations

The Government of India should consider international and UN mechanisms and accept certain important international human rights mechanism, like the UN Special Procedures and treaty bodies. It is important not only to protect and promote its human rights but also to continue to play a leadership position in persuading other developing countries.

There is also an urgent need for the NHRC and the State Human Rights Commissions to have more independence and power of enforcement in particular to ensure their “recommendations”.

It is recommended that administrative and law enforcement officials be provided with guidance, directives and training to uphold FoE online and offline.

Recommendations

It is recommended that law enforcement authorities be held liable and accountable for human rights violations by an independent and democratic oversight body and court of law.

It is recommended that individuals and communities should be able to seek financial and other resources, in a timely, equitable, transparent and accountable manner to exercise their FoE rights.

It is recommended that consistent oversight of blocking of internet based content by competent authority be set up on a regular basis so that arbitrary actions are ruled out.

It is recommended that victims of violations and abuses to rights of FoE have the right to effective remedy and redress in the court of law.