State of Internet Rights and Freedom in India
February 4th, 2015
India International Centre, Lecture Hall 2, Annexxe, New Delhi

Consultation brief

DEF held a consultative meeting on Internet Rights project with APC-IMPACT Advisory Committee members, think-tank and academic institutions, independent consultants, staff at European Union and civil society groups. The objective of the consultative meeting was present the secondary research conducted around the Frank La Rue Framework concerning Freedom of Expression online in India.

DEF research team explained the country-level research methodology and Frank La Rue framework to the members of the consultation. It included a preliminary mapping of laws, policies and cases of violations around the checklist factors in India. Based on the preliminary research, consultation will be followed by one-on-one meetings with experts, email and phone interviews and survey research across the 100 DEF's Community Information Research Centres across India.

Some of the broad observations and feedback received from the consultation include:

I. **Title:** The title, "State of Internet Rights and Freedom in India" should be carefully examined and defined properly, as Internet Freedom and Freedom of Expression online have varied connotations. In this context, the report should mention that it looks into FoE, both online and offline

II. **FLR checklist:** Members recommended that the country report define specific terms in the FLR checklist, as the meaning may be perceived and treated differently in the Indian context. Some of the terms in the checklist include:

a) **Freedom of Expression:** Examining just the right to freedom of expression by individuals may be one sided because the Indian constitution guarantees these rights, but with reasonable restrictions.

- **Protecting FoE online:** The FLR checklist mentions affording and protecting Freedom of Expression online, but does not mention the roles and responsibilities of individuals to exercise these rights. Furthermore, the report should also mention the Preamble of the Indian Constitution.

    - **Comment:** While these rights apply both offline and online, the Indian constitution does mention that no law shall be made that goes against the constitution

- **Section 66A and 69A of the IT Act:** These sections are frequently being misused, in addition, to the Constitutional restrictions. These restrictions pose a problem as these contradict our constitutional values. Therefore with the use of laws such laws the balance between the fundamental rights

and fundamental duties gets disturbed. For example, a closer look at the cases where 66A and 69A have been invoked, 80 to 90% of cases are related to stifling of political opposition. In those cases there is no threat to the defense of the country, but rather disagreeing with a Chief Minister of a state or a particular policy

- **Section 295A and 153A of the Indian Penal Code:** These sections should be incorporated in the FLR checklist because they relate to the IT Act, however, it does not mention explicitly the online aspects of FoE

- **Access:** The debate in India should be focused on access, because it is a violation of human right if communities lack access to internet. Without access, communities cannot exercise their human rights online

    - **Comment:** Concrete and effective policy is developed with public and private sector to make the internet available, accessible and affordable to all: Policies are formulated to make internet available, accessible and affordable in India, however, the report should aim to identify the gaps and challenges in implementation

b) **Content Blocking under Indian Telegraph Act:** The report should also look at Indian Telegraph Act, 1885, along with IT Act. Blocking is done via Telegraph Act. Broadly, after a complaint is made to DIT, the government body identifies what has to be blocked and then in turn asks Department of Telecom to block the content. So blocking is done under Indian Telegraph Act and not IT Act because all licenses are given under section 4 of Indian Telegraph Act 1885 which gives reason to study the Telegraph Act.

- **Comment:** The reason why "arbitrary blocking" phrase was used in FLR checklist is because that was one of the criteria that Frank La Rue used in his report to assess whether or not restrictions on FoE were acceptable or not. Further, he didn't say blocking is never justified. La Rue believed that in some cases arbitrary blocking is justified. Different organisations have been using FLR report to assess the state of internet rights in different countries. APC has basically developed checklist based on that report (used by New Zealand) - systematic way of comparing situations in different countries (using FLR framework) that is not to say extra criteria cannot be incorporated.

- **Comment:** There are two aspects to blocking - one is, there is blocking which is desired by the state and imposed upon the service provider to carry out the blocking - they have no choice. In that context, within the FLR framework, cases should be highlighted where blocking is justified and where it is not justified. Also, in some cases because of some technical issue, specific content could not be banned, so the entire website is blocked

- **Comment:** There is Gazette notification that describes how the content was blocked

c) **Generic Bans on Content:** There are "no generic" bans on content: There are generic bans on content in India. However, the term "generic ban" should be defined within the report.

- **Comment:** Child pornography is an example of generic ban. It is never allowed. But individual banning of sites may not be considered a generic ban as the banning is temporary and when issue gets settled, site can be accessed again. But individual banning of sites may not be considered a generic ban as the banning is temporary.

d) **Criminalizing Legitimate Expressions:** There is a real problem in India, where the security apparatus lets go off people causing violence. So, the solution to the problem is not restriction on FoE or Freedom of Association because India is a complex. In exceptional cases of crisis restriction may be legitimate but in most cases it is not legitimate and there is no need to legitimize it by calling India a complex society.

- **Comment:** Government should proactively disseminate information without asking for it. Information should not be shared only when it is asked for or by going to court.

- **Comment:** Business houses or powerful social groups are guilty than the state and it is more difficult to hold them accountable.

- **Comment:** Not many corporate news organisations support or back their employees. They simply remove or block information/article--so we should look at these cases. (i.e. Tamil Nadu Author Perumal Murugan who committed internet suicide)

e) **Monitoring and Surveillance:** "State doesn't regularly track the online activities of human rights defenders, activists and opposition members". There is open evidence that state does monitor data. Secondly, does it gather meta-data? Yes, it does. For example, some principles of NATGRID project, NATGRID project was supposed to look at meta-data and for this the government is connecting data bases that is already available and most of it is digital data or databases which are being digitized and therefore, they are creating a platform where all the data is available

- **Comment:** Real name registration policies. State does not "adopt" real name registration policies: An alternative term should be incorporated. India "enforces" real name registration policies

- **Comment:** There are two concerns: data and surveillance. This helps to automatically look at surveillance concerns and databases that does not involve national security concerns like corporate data processing

- **Comment:** There are some countries that have to disclose details to the person under surveillance within a legally mandated time frame. Estonia, for example, if some institution or body seeks individual (personal) data, the entity has to provide reasons as to why personal data is being asked for.

After some time, there is a disclosure report that has to be submitted as well.

- **Comment:** National security and surveillance issues should be addressed separately

- **Comment:** Study the principle that originated out of the US Surveillance Jurisprudence. "Reasonable Expectation of Privacy" in the "Cats vs. United States" Here, the case didn't give any mathematical or precise test of what would amount to invasion of privacy, but instead, it talked about a reasonable expectation of privacy, which the law would expect is an expectation that will have both a subjective expectation of privacy and an objective expectation of privacy. For example, subjective expectation of an individual to treat something about his/her life as private and society should be willing to treat that as private. (i.e. private individual's sex life). However, Nira Radia's conversation on the phone – in this case Nira Radia may think or feel that her conversation should be treated as private but society may not think so. So, this is not a precise test but that is where the law stands now.

- **Comment:** One should focus on the lack of transparency of the government and its processes because if one is talking about invasion of privacy, citizens end up being very transparent unlike the government. So, the more the government is transparent, the more faith citizens will show when sharing data.

f) **Cyber-attacks: Define cyber-attack?**

- **Comment:** Look at cyber-attacks as Computer Network Exploitation - brought out by Snowden. A state may be justified in carrying out surveillance but it is a cyber-attack on whom it is being carried out. So when state, even for purposes of surveillance, espionage, gathering intelligence etc., it is actually a form of cyber-attack on the other.

- **Comment:** There are different types of cyber-attack(s): one is offensive. Are there any rules that prevent states from carrying out such offensive attacks? But it is difficult to track such cases as such attacks are done by third parties.

- **Comment:** Anonymity is being questioned. For example, if one needs a Gmail account, he or she will have to go through some form of authentication process, like by giving mobile numbers and it is through such processes one may not end up being anonymous

g) **Multistakeholderism:** State participates in "multistakeholder" initiatives to protect human rights. India may participate in multilateral initiatives, but how do we look at "multistakeholderism" in the country report? Does this mean at the national, regional or international level? Identify the stakeholders**?**

- **Comment**: India makes its positions known on economic, social and cultural rights at international forums, but, is silent on matters related to civic and political matters.

- **Comment**: UN Human rights council is a multilateral forum and not multi-stakeholder forum. Being a member of UNHRC does not demonstrate the Indian government's commitment and position on human rights. India, at the UNHRC, supports resolutions around social and economic rights and on sovereignty of states. However, India is weak on supporting resolutions that are on political and civil rights and this is definitely true for the online sphere. So the question is not just that India is present at UNHRC meetings, but rather, what position the country takes on relevant human rights issues

- **Comment**: There is a difference between multi-stakeholder initiatives and multi-lateral initiatives. IGF, for example, is one multi-stakeholder initiative, that is relevant to the topic. And multi-lateral initiatives are many related to the human rights. So, the report needs to distinguish between what India is signatory to and related to FoE online. In the 2012 HRC session, India was a co-sponsor on FoE online, but later India was not a co-sponsor.

- **Comment on Internet Governance:** At the International Telecommunication Union meeting in October 2014, India was trying to challenge the multi-stakeholder governance approach of the internet and argued in favor of sovereign control of the internet and identification of users using the internet and content. With this sort of mindset and approach - the privacy of citizens is under threat and multi-stakeholder approach of governance of internet is also subject to challenge

- **Comment on transparency from the Indian government:** Within the context of public consultation, India holds public consultations with stakeholders, but, the process often lacks transparency. For example, only a certain group(s) of civil society groups are given access to the consultation. The nature of the consultation, its place and time is often unknown. The outcomes are even less known. For example, Multistakeholder Advisory Group has been formed, but, the outcomes of the proceedings are not available readily.

h) **Net Neutrality:** Incorporate Net Neutrality in the checklist as it relates to internet availability, accessibility and affordability

i) **Women's Rights:** There are laws that try to protect women and their dignity online and the applicability of these laws online. But the question is whether they are sufficient to protect women online. The recommendation is to look at the laws separately and how they operate in the online world

- **Comment:** Look at the cases being reported and whether the cases are being reported freely

- **Comment:** Check whether offline laws apply online as well and study how culture offline influences behavior online

- **Comment:** Along with women's' issues, we should also look at other categories like S.C, S.Ts, LGBT.

III. Laws and policies: Members recommended (additional) studying the legal instruments:

a) Sections around Freedom of Expression in the Indian Constitution

b) Sections of the IT Act

- Sec 67B
- Sec 67
- Sec 67A
- Sec69A

c) Indian Telegraph Act

- Section 5 of the Telegraph Act – lays out certain conditions for the legitimate ways for the state to carry out the surveillance. And in this context, it is important to make a distinction between targeted and mass surveillance

d) Blocking Rules

e) Intermediary Guidelines

f) Indian Penal Code

g) Case laws to monitor:

- R. Raja Gopal vs. Tamil Nadu

- 1996 Judgment in the case of PUCL vs. India: Targeted telephone surveillance under the Telegraph Act and in this case Supreme Court mandated guidelines and Section 4 (19) (A) was updated

- Ratan Tata's case on privacy

- Kamlesh Vaswani vs. Union of India

IV. Research, International Mechanisms and Best Practices to examine:

a) Surveillance and Privacy paper published by Internet Democracy Project
b) Open Net Initiative Research
c) European Union Committee on Legal Affairs and Human Rights report
d) South Korea's Anonymity Project (similar to UID in India) and UK surveillance law—DRIP
e) Canadian experience on privacy and surveillance

Annexure1: List of Participants

Sr. No	Name	Title, Organization
1	AK Goyal	UNESCO, Cornicle
2	Amitabh Dubey	Director, Trusted Sources
3	Amitabh Singhal	Member, APC-IMPACT Advisory Committee
4	Anja Kovac	Director, Internet Democracy Project and Member, APC-IMPACT Advisory Committee
5	Anurag Vibhuti	Assistant Director, Telecom Centers of Excellence India
6	Arjun J	Software Freedom Law Centre
7	Arjun Sen	Consultant, DEF
8	Deepak Maheshwari	Head, Government Affairs at Symantec and Member, APC-IMPACT Advisory Committee
9	Gangesh S Varma	Research Scholar, Center for International Legal Studies, JNU
10	Geetha Hariharan	CIS
11	Maubani Dutta	Research Associate, DEF
12	Niki A. Shah	Program Officer, DEF
13	Osama Manzar	Founder-Director, DEF and Member, APC-IMPACT Advisory Committee
14	Pradeep Singh	DEF
15	Rahul Choudhary	Computer Science Engineer, DEF
16	Rahul Gupta	Research Coordinator, Telecom Centres of Excellence India
17	Rajat Kumar	Coordinator-Research & Advocacy
18	Rajat Kumar	Research Associate, DEF
19	Renuka Srinivasan	Programme Manager, Delegation of the European Union to India
20	Ritu Srivastava	Program Manager, DEF
21	Saikat Dutta	Editor (National Security), HT Media Ltd and Member, APC-IMPACT Advisory Committee
22	Shivani Lal	Research Associate, Working Groups on Human Rights
23	Srikanth Chandrasekaran	Senior Manager, IEEE
24	Syed Kazi	Deputy Director, DEF and Member, APC-IMPACT Advisory Committee
25	Ujwala Uppaluri	Research Fellow, Center for Communication Governance, National Law University , Delhi