# UNESCO's Comprehensive Study on Internet Related Issues

**Submitted by :**

**Name:** Prasanth Sugathan

**Gender:** Male

**Category of Stakeholder:** A. civil society and NGOs including individual users

**Country:** India

**Region:** Asia and the Pacific

1. **What can be done to reinforce the right to seek and receive information in the online environment?**

Freedom of speech and expression includes the right to express as well as the right to seek and receive information. However, this freedom is often curtailed due to censorship, private take-down mechanisms and legislations that treat online content differently from offline content. There is a need to develop a broad consensus internationally on ensuring the right to access the Internet to people across the world.

2. **What mechanisms can develop policies and common standards for open-licensed educational resources and scientific repositories, and for the long-term preservation of digital heritage?**

Open-licensed content can go a long way in reducing the entry barriers to gain knowledge and can faciltate the process of improving standards of education across the world. There should be greater thrust on making available content in regional languages. The role of community initiatives like that of Wikipedia and the Free Software Community could be utilised in achieving goals like greater regional content and translation of content. There should also be greater empasis on utilising and expanding fair use provisions to enable use of copyrighted material for educational purposes.

3. **How can greater progress be made as regards inclusive strategies for women and girls as well as marginalized and disabled people?**

4. **How can accessibility be facilitated through increases in locally produced and relevant content in different languages?**

Governments and civil society have a major role to play in producing relevant content in different languages, especially languages that have lesser number of native speakers.

Community initiatives need to be strengthened to ensure creation of content in different languages. This is important to preserve the rich heritage of various regions and to ensure more people gets access to online content.

**5. What can be done to institutionalize Media and Information Literacy (MIL) effectively in national educational systems?**

**6. What are the current and emerging challenges relevant to freedom of expression online?**

Below is a non-exhaustive list of current and emerging challenges that impact freedom of expression on-line:

Intermediary liability: While some jurisdictions do offer crystallized safe-harbor protections to Internet intermediaries against liability arising from content that is user-generated, but hosted, stored or transmitted by intermediaries, the law in this regard is somewhat haphazardly developed in others. In India for instance, the Information Technology Act 2000 as a general rule exempts intermediaries from liability for user-generated content. However, this exemption is contingent upon the intermediaries' observance of certain “due-diligence” criteria as laid down by the Information Technology (Intermediaries Guidelines) Rules 2011. As part of due-diligence, the Rules (in broad and ambiguous terms) identify an immensely broad gamut of “unlawful” content that intermediaries have to take down on being notified by an aggrieved person, and failure to observe due-diligence will result in forfeiture of safe-harbor protection offered by the Act. Further, the Act and Rules offer no avenues for put-back of content that was wrongfully taken-down as unlawful. This uncertainty regarding content that may be termed unlawful, coupled with the imposition of adjudicatory roles on intermediaries that they are ill-equipped to handle, results in a chilling effect on free speech – firstly as users must exercise extreme caution over content they upload lest it be taken-down as unlawful; and secondly as intermediaries face a perpetual threat of prosecution over content that was misidentified as lawful and allowed to remain on-line.

Similar lacunae in intermediary liability law exist in several jurisdictions across the world, limiting the individual's right to free speech in the process. The formulation and adoption of a set of universal principles that ensure justice and equity in intermediary regulation would be a commendable start to remedying this state of affairs. Furthermore, nations must solidify their laws governing intermediary liability, and said laws must ideally be uniform across jurisdictions in light of the border-less nature of the Internet. Take-down and put-back mechanisms for user-generated content must be available and well-defined, must offer no room for ambiguity or misuse, and most importantly, must carefully balance the interests of all relevant stakeholders. Intermediaries should not be forced to adjudicate on the lawful nature of user-generated content and such decisions should only be made by the judiciary.

State surveillance: Ever since Snowden's paradigm-altering revelations on state surveillance programs back in June 2013, striking a long-term balance between the state's obligation to

safeguard national security on the one hand, and the citizens' rights to privacy and free speech on the other, has generated much debate in policy circles world over. Seeing how invasive surveillance initiatives inevitably compromise citizens' civil liberties despite being powerful tools to safeguard national security, states have the added responsibility of keeping the incidence on civil liberties to a bare minimum and allaying legitimate public concerns in this regard. While the former of these responsibilities can be met by states' review and restructure of internal surveillance frameworks around strict accountability norms, the latter calls for a more open and inclusive approach towards surveillance, including by allowing public scrutiny of surveillance frameworks to the extent possible without compromising functionality.

However, this is hardly the current practice. In India, next to no information on the executive-driven surveillance machinery is publicly released, and formal requests for information made under the Right to Information Act are mostly denied citing legislative exemption due to national security concerns. This is cause for concern especially since India has yet to accord legislative recognition to a right to privacy, and there is no independent oversight – judicial or otherwise – of state surveillance whatsoever.

Internet censorship: Despite the Internet being an open global network with its foundations in the free flow of information, several jurisdictions across the world attempt to control what can be accessed or published on the Internet. Such restriction of access, though founded in a broad range of concerns ranging from national security to protection of cultural and moral values, invariably result in curtailment of the individual's right to freedom of speech and expression. In India, the Government reserves the right under the Information Technology Act to block content on the Internet from public access in the interest of security, public order etc. However, there is little transparency in the procedure surrounding such blocking of content, and reasons behind specific instances of blockage are never disclosed. There have also been instances where entire websites were blocked in place of specific URLs. More recently, the Government of India has been contemplating the installation of nation-wide filters to block access to pornographic content on the Internet, and petitions currently pending before the Supreme Court and Parliament have even prayed for the criminalization of porn-viewership.

**7. How can legislation in a diverse range of fields which impacts on the Internet respect freedom of expression in line with international standards?**

**8. Is there a need for specific protections for freedom of expression for the Internet?**

Many jurisdictions treat online content differently from offline content with legislations often prescribing harsher punishment for "unlawful" content published online. In India, for instance, Section 66A of the Information Technology Act, 2000 prescribes a punishment of upto three years imprisonment for sending offensive messages through communication service. The provision uses very broad, undefined terms resulting in the abuse of the provision by law enforcement agencies. Thus, if not a special protection for online speech, there is certainly a need to at least treat online speech to be on par with offline speech.

9. **To what extent do laws protect digitally interfaced journalism and journalistic sources?**

10. **What are the optimum ways to deal with online hate speech? How can Media and Information Literacy empower users to understand and exercise freedom of expression on the Internet?**

11. **What are the optimum systems for independent self-regulation by journalistic actors and intermediaries in cyberspace?**

12. **What principles should ensure respect for the right to privacy?**

The International Principles on the Application of Human Rights to Communications Surveillance articulate what international human rights law require of governments in the digital age. They speak to a growing global consensus that modern surveillance has gone too far and needs to be restrained. They also give benchmarks that people around the world can use to evaluate and push for changes in their own legal systems. The product of over a year of consultation among civil society, privacy and technology experts, the principles have already been co-signed by over hundred organizations from around the world. The process was led by Privacy International, Access, and the Electronic Frontier Foundation. Though the principles given below are directed at oversight of communications surveillance in particular, they are equally applicable to a broader right to privacy:

Legality: Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.

Legitimate aim: Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Necessity: Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

Adequacy: Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific Legitimate Aim identified.

Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;

There is a high degree of probability that evidence relevant and material to such a crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought, and;

Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option, and;

Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged, and;

Any excess information collected will not be retained, but will be instead promptly destroyed or returned, and;

Information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given, and;

That the surveillance activities requested and techniques proposed do not undermine the essence of right to privacy or of fundamental freedoms.

Competent judicial authority: Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

Separate and independent from the authorities conducting communications surveillance

Conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights

Have adequate resources in exercising the functions assigned to them

Due process: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by

law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.

User notification: Those whose communications are being surveilled should be notified of a decision authorizing Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstance:

Notifications would seriously jeopardize the purpose for which the communications surveillance is authorized, or there is an imminent risk of danger to human life; and

Authorization to delay notification is granted by a competent judicial authority; and

The user affected is notified as soon as the risk is lifted as notified by a competent judicial authority

The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

Transparency: States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.

Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. Oversight mechanisms should have the authority: to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

Integrity of communications and systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes. A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users.

Safeguards for international cooperation: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

Safeguards against illegitimate access and right to effective remedy: States should enact legislation criminalizing illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle-blowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.

**13. What is the relationship between privacy, anonymity and encryption?**

**14. What is the importance of transparency around limitations of privacy?**

Seeing how privacy-limiting measures usually enable access to sensitive personal information that individuals have strong incentives to keep private, it is extremely important that they be as transparent as possible. Opacity in privacy-limiting measures gives room for legitimate concerns that they are not implemented with the levels of caution required to ensure the security of personal information accessed, and when said opacity occurs in measures that also carry force of law i.e. when individuals do not have the option of non-association with the privacy-limiting measures, it leads to decline in trust in state-action.

15. **What kinds of arrangements can help to safeguard the exercise of privacy in relation to other rights?**

16. **How can openness and transparency of data be reconciled with privacy?**

17. **What may be the impact of issues relating to big data on respect for privacy?**

18. **How can security of personal data be enhanced?**

19. **How can Media and Information Literacy be developed to assist individuals to protect their privacy?**

20. **How can ethical principles based on international human rights advance accessibility, openness, and multi-stakeholder participation on the Internet?**

21. **What conceptual frameworks or processes of inquiry could serve to analyse, assess, and thereby inform the choices that confront stakeholders in the new social uses and applications of information and knowledge?**

22. **How does ethical consideration relate to gender dimensions of the Internet?**

23. **How can ethics, - i.e. the simultaneous affirmation of human rights, peace, equity, and justice - inform law and regulation about the Internet?**

24. **What international, regional and national frameworks, normative guidelines and accountability mechanisms exist of relevance to one or more fields of the study?**

With reference to limitation of free speech on-line through intermediary liability laws, the relevant global legal framework includes:

Directive 2000/31/EC [European Union]

Classifies intermediaries based on function and provides safe-harbor protection against liability arising from user-generated content

The Electronic Commerce (EC Directive) Regulations, 2002 [United Kingdom]

Transposes Directive 2000/31/EC to UK law

Communications Decency Act [United States of America]

Section 230 provides immunity to intermediaries against user-generated content by not treating them as publishers of content

Digital Millennium Copyright Act [United States of America]

Lays down the procedure for take-down of copyright infringing content

Copyright Act, 1968 [Australia]

Classifies Internet intermediaries based on function and provides immunity against user-generated content to internet service providers

Copyright Regulations, 1969 [Australia]

Mandates the procedure for take-down of content that infringes copyright

Broadcasting Services Amendment (Online Services) Act, 1999 [Australia]

Authorizes the Australian Communications and Media Authority to regulate Internet content and issue take down notices on receiving complaints from individuals

Marco Civil da Internet [Brazil]

Provides safe-harbor protection to intermediaries and requires intermediaries to take down content on receipt of a court order

Information Technology Act, 2000 [India]

Section 79 offers limited safe-harbor protection to Internet intermediaries against liability arising out of user-generated content

Information Technology (Intermediaries Guidelines) Rules, 2011 [India]

Rule 3 outlines the due-diligence criteria, upon the observance of which safe-harbor protection under Section 79 of the Act is contingent. It also lays down the procedure for take-down of content deemed unlawful.

Apart from these legislations, the issue of intermediary liability has also been addressed by independent studies, including:

Report of the UN Special Rapporteur (Frank La Rue) on the Promotion and Protection of the Right to Freedom of Opinion and Expression, available at:

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

“Internet Intermediaries: Dilemma of Liability” - a policy brief on intermediary liability developed by Article 19, available at:

http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

**25. How do cross-jurisdictional issues operate with regard to freedom of expression and privacy?**

**26. What are the intersections between the fields of study: for example, between access and freedom of expression; ethics and privacy; privacy and freedom of expression; and between all four elements?**

**27. What pertinent information materials exist that cut across or which are relevant to the four fields of the study?**

Below is a link to a report by SFLC.in titled “Information Technology (Intermediaries Guidelines) Rules, 2011: An Analysis”. This report, drawing from multiple Round Table Consultations we organized across India, contains a detailed analysis of India's legislative regulation of on-line intermediaries and lays down nine fundamental principles that we feel must govern an ideal liability regime. The report also contains cross-jurisdictional analyses of intermediary liability regimes and stakeholder recommendations towards improving the current framework of regulation.

http://sflc.in/information-technology-intermediaries-guidelines-rules-2011-an-analysis-2/

SFLC.in has also published a report on Indian communications surveillance, where we take an in-depth look at the various legal and procedural frameworks governing surveillance. The report also builds descriptive profiles India's surveillance programs such as the Central Monitoring System and Network Traffic Analysis, and examines the broad surveillance framework for compliance with international principles. The report titled “India's surveillance state” is available at the link below:

http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf

**28. What might be the options for role of UNESCO within the wider UN system in regard to the distinct issues of online Access to information and knowledge, Freedom of Expression, Privacy and Ethical dimensions of the information society?**

**29. What might be options for the role of UNESCO in relation to stakeholders outside the UN system?**

**30. For each study field, what specific options might UNESCO Member States consider?**