Frank La Rue (FLR) Framework for Freedom of Expression

Area	Checklist	Y/N/U	Law & Policy in India: Y/N	Policy or Law	Cases Monitored	Analysis	Recommendations
Laws and Policies that are applicable to the internet	**Section 66A** of the IT Act- Punishment for sending offensive messages through communication service, etc. Any person who sends, by means of a computer resource or a communication device,— (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device, (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine. **Section 69A** of the IT Act- Power to issue directions for blocking for public access of any information through any computer resource.- (1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource. (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed. (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine. **Section 295 of the IPC** - Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs.—Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of 273 [citizens of India], 274 [by words, either spoken or written, or by signs or by visible representations or otherwise], insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to 4[three years], or with fine, or with both. **Section 153A** of the IT Act- Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.— (1) Whoever— (a) by words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities, or (b) commits any act which is prejudicial to the maintenance of harmony between different religious, racial, language or regional groups or castes or communities, and which disturbs or is likely to disturb the public tranquility, 2[or] 2[(c) organizes any exercise, movement, drill or other similar activity intending that the participants in such activity shall use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, or participates in such activity intending to use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force							

	or violence, against any religious, racial, language or regional group or caste or community and such activity for any reason whatsoever causes or is likely to cause fear or alarm or a feeling of insecurity amongst members of such religious, racial, language or regional group or caste or community,] shall be punished with imprisonment which may extend to three years, or with fine, or with both. Offence committed in place of worship, etc.—(2) Whoever commits an offence specified in sub-section (1) in any place of worship or in any assembly engaged in the performance of religious wor¬ship or religious ceremonies, shall be punished with imprisonment which may extend to five years and shall also be liable to fine. **Section 79A** of the IT Act- Central Government to notify Examiner of Electronic Evidence.- The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. **Kamlesh Vaswani v. UoI [W.P.(C).No. 177 of 2103]** This writ petition was filed before the SC under Article 32 of the Constitution of India in public interest challenging Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act 2000 (hereinafter referred to as the Act) as unconstitutional, as they are inefficient in tackling the rampant availability of pornographic material in India. The petitioner submits that the porn industry has become a big profit making machine. Advertisements of pornographic websites are often displayed without the permission of viewers. Such uncontrolled displays of porn usually occur while browsing the internet at home or at business meetings and this is extremely offensive to the viewers. It is the petitioner's opinion that pornography is a moral cancer that corrupts our social values every second across the country. More importantly, the term 'pornography' has not been defined in any Statute. This leads to non-recognition of problems such as child pornography, virtual pornography, poser pornography, as well as crimes against women/girls/children that are mostly fueled by pornography. The petitioner further submits that the respondents are to ensure the protection of all women/ children, and the prosecution/punishment of all offenders. They are also to ensure the proper psycho-social counseling and rehabilitation of victims, and education of all women/children. But the respondents have failed to enforce even the existing laws, to the detriment of rights of members of society to lead a peaceful moral life. Existing provisions within the IT Act that purport to tackle the menace of pornography/cyber crimes – namely Sections 66,67, 69, 71, 72, 75, 79 and 80 – fail to do so since the Act is primarily meant to promote e-commerce and e-governance and is resultantly inefficient in tackling cyber crimes. Further, the petitioner suggests that in metropolitan cities (such as Delhi, Mumbai, Kolkata and Chennai), investigating officers should immediately inspect cyber cafes to determine whether porn videos are being made available. If yes, they should immediately be seized. **Section 67B of the IT Act**- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.- Whoever,- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) facilitates abusing children online or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the

	event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or (ii) which is kept or used for bonafide heritage or religious purposes. **Section 67 of the IT Act** - Punishment for publishing or transmitting obscene material in electronic form. -Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees. **PUCL PIL challenging validity of a section in the Telegraph Act, 1885** - There have been a number of articles on the Cabinet Secretary's report regarding tapping of telephones which appeared in some section of the media. It is important that the correct factual position is presented to the media. The provisions for authorization of interception are contained in Section 5(2) of Indian Telegraph Act, 1885 read with Rule 419(A) of the Indian Telegraph Rules, 1951 as well as Section 69 of the Information Technology Act, 2000 read with Information Technology (Directions for Interception or Monitoring or Decryption of Information) Rules, 2009. The Hon'ble Supreme Court has upheld the constitutional validity of interceptions and monitoring under Section 5(2) of the Act through its order dated 18.12.1996 in Writ Petition (C) No.256/1991 by People's Union for Civil Liberties (PUCL) Vs. Union of India. It has also observed that the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "Right to Privacy", and accordingly, held that telephone tapping would infringe the Right to Life and Right to Freedom of Speech & Expression enshrined in Articles 21 and 19(1)(a) respectively of the Constitution of India, unless it is permitted under the procedure established by law. The Hon'ble Court further observed that Section 5(2) of the Act clearly provides that 'occurrence of any public emergency' or 'interest of public safety' is a sine qua non for the application of these provisions. Neither of these are secretive conditions or situations. Either of the situations would be apparent to a reasonable person. In this regard, the Hon'ble Court has recalled its observations in the case of Hukum Chand Shyamlal Vs. Union of India and others, 1976 stating that 'economic emergency' is not one of those matters expressly mentioned in the statute, and further that mere 'economic emergency' may not necessarily amount to a 'public emergency' and justify action under Section 5(2) of the Act, unless it raises problems relating to the matters indicated in the section. 'Public emergency' would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. It is one which raises problems concerning the interest of public safety, the sovereignty and integrity of India, the security of the State, friendly relations with sovereign States or public order or the prevention of incitement to the commission of an offence. 'Public Safety' means the state of condition of freedom from danger or risk for the people at large. It has been stated further that when either of these two conditions are not in existence, authorities cannot resort to telephone tapping, even though there is satisfaction that it is necessary or expedient to do so in the interests of sovereignty and integrity of India, security of the State, friendly relations with sovereign States, public order or for preventing incitement to the commission of an offence. In the light of the above, the Hon'ble Supreme Court gave directions covering the issue of institutional safeguards to be put in place in respect of

	interception under Section 5(2) of the Indian Telegraph Act, which was incorporated in terms of Rule 419(A) of the Indian Telegraph Rule, 1951. In the light of recent controversies on account of interception of certain telephone numbers by a designated authorized agency, which were extensively reported by media, the Hon'ble Prime Minister directed the Cabinet Secretary to look into the Rules, Procedures and Mechanism to avoid their misuse. After examining all the relevant issues, Cabinet Secretary recommended further comprehensive refinement of Rules and Procedures, in addition to providing for stronger penal provisions for violations by amending the law. It was also recommended to either remove the CBDT from the list of authorized agencies in respect of telephone interception as the income tax laws fall within civil jurisdiction and do not always impinge on the public safety or to specify stipulations regarding the extent of surveillance allowed to the agency, including the level at which requests are to be made for authorization by the Home Secretary. It is clarified that the law does not permit use of telephone tapping and monitoring of conversations to merely detect tax evasion. There are specific laws and rules that contain provisions for detection of unaccounted wealth and evasion of taxes, and interception of telephones without 'public emergency' or 'public safety' being at stake is not in accordance with the law, as exhaustively interpreted by the Hon'ble Supreme Court. The recommendations made by the Cabinet Secretary reiterate this established legal position, which should not be seen in terms of conflicts between individuals or interest groups. **R. Rajagopal vs State Of T.N on 7 October, 1994 -** The Judgment of the Court was delivered by B.P. JEEVAN REDDY, J.- This petition raises a question concerning the freedom of press vis-A-vis the right to privacy of the citizens of this country. It also raises the question as to the parameters of the right of the press to criticise and comment on the acts and conduct of public officials. **Katz versus United States -** Acting on a suspicion that Katz was transmitting gambling information over the phone to clients in other states, Federal agents attached an eavesdropping device to the outside of a public phone booth used by Katz. Based on recordings of his end of the conversations, Katz was convicted under an eight- count indictment for the illegal transmission of wagering information from Los Angeles to Boston and Miami. On appeal, Katz challanged his conviction arguing that the recordings could not be used as evidence against him. The Court of Appeals rejected this point, noting the absence of a physical intrusion into the phone booth itself. The Court granted certiorari. **Section 5(2) in The Indian Telegraph Act, 1885 -** On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: tc "(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order\:" Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.] tc "Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless

	their transmission has been prohibited under this sub-section						
General protection of freedom of expression	National constitution or laws protect internet-based freedom of expression.	Y	Yes	Article 19 of the Indian ConstitutionIT Act	There have been a number of cases where individuals have been detained or arrested invoking Section 69A of the IT Act during the 2013-2014 calendar year, according to Freedom on the Net Report issued by Freedom House.	Article 18 and 19 protects freedom of speech and expression, but does not explicitly mention internet-based freedom. The practical implication of Section 66A of the IT Act (2008) and its legality is widely debated among stakeholdersThe Indian constitution guarantees freedom of expression, however, the IT Act 2011 may be amended to explicitly define internet-based FoE and what the government deems as offensive communications, in the context of protecting national security or other sovereignty/territorial issues.Human Rights resolution 21/16 Paragraph 1 states of the (states) obligation to respect and fully "protect the rights of all individuals to assemble peacefully and associate freely, online as well as	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.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.

						offline."	
	State participates in multi-stakeholder initiatives to protect human rights online.	U	No		GOI participated in the Internet Governance Forum held on 2-5 September 2014 in Istanbul, Turkey.	The Indian government participated in the Internet Governance Forum	It is important to differentiate between multi-stakeholder initiatives and multilateral initatives
	Restrictions on online content	Y	Yes		Procedure and Safeguards for Blocking for Access of Information by Public) "Blocking Rules" Section 66A of the IT Act Section 69A of the IT Act	130 court orders to block web content were received by the Information ministry between February 2009 and December 2013. Blocking of websites take place under Section 69A of the IT Act. The rules empower the central government to direct any agency or intermediary to block access to information when it is satisfied to do, in the interest of "sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence Kamlesh Vawani Case.	Currently, there is no law in India against viewing pornography. However, both laws prohibit producing and transmitting "obscene material."
Arbitrary blocking or	There are no generic bans on	Y	Yes	IT Act	For example, under the Customs Act, it	The law prohibits content that could	Content Blocking under Indian Telegraph Act: The report should

filtering	content			Procedure and Safeguards for Blocking for Access of Information by Public) "Blocking Rules"	remained illegal to import Salman Rushdie's book, The Satanic Verses Child Pornography is an example of Generic Ban.	harm religious sentiments or provoke enmity among groups. State governments banned some books from being imported or sold in the state because they contained material that government censors deemed inflammatory and apt to provoke communal or religious tensions. 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. 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	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.

						banning of sites may not be considered a generic ban as the banning is temporary.	
	Sites are not prohibited solely because of political or government criticism	No	Yes	IT Act Procedure and Safeguards for Blocking for Access of Informatio n by Public) "Blocking Rules"	In the national elections, reports about online content manipulation did surface, but discourse and online campaigning remained strong on all sides. In June 2013, some ISPs were blocking at least two image hosting websites and a political log hosed on UK-based service, however, the reasons for these blocks is unknown.	Blocking of websites take place under Section 69A of the IT Act. The rules empower the central government to direct any agency or intermediary to block access to information when it is satisfied to do, in the interest of "sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence	Sites are not prohibited solely because of political or government criticism
	State blocks or filters websites based on lawful criteria	U	Yes	IT Act Procedure and Safeguards for Blocking for Access of Informatio n by Public) "Blocking	The Indian government, in 2013, issued orders to varilus companies like Google and Facebook, among others to block content. Whether a criteria exists to evaluate to block or filters websites is unclear. However, in the interest of	There is a process within the government for how content is blocked or websites are ordered for blocking. According to the Freedom on the Net report, the "scale of blocking is consequently difficult to assess.	§ 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. § 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

				Rules" Intermediaries Guidelines 2011 Indian Teleraph Act, 1885 Section 295A and Section 153A used in conjunction with 66A. Section 79A. Section 69A Section 67B Section 67A	national security and other natinal matters to protect sovereignty, the Indian government does block websites	In March 2013, a parliamentary standing committee recommended clearer definition of prohibited content expressing concern that the ambiguity could lead to censorship without due process and harassment of intermediaries	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
	State blocks or filters websites based on lawful criteria	U	Yes	IT Act Procedure and Safeguards for Blocking for Access of Information by Public)	The Indian government, in 2013, issued orders to varilus companies like Google and Facebook, among others to block content. Whether a criteria exists to evaluate to block or filters websites is	There is a process within the government for how content is blocked or websites are ordered for blocking. According to the Freedom on the Net report, the "scale of blocking is consequently difficult to assess.	§ 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. § 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 -

				"Blocking Rules" Intermediaries Guidelines 2011 Indian Telegraph Act, 1885 Section 295A and Section 153A used in conjunction with 66A. Section 79A. Section 69A Section 67B Section 67A	unclear. However, in the interest of national security and other national matters to protect sovereignty, the Indian government does block websites	In March 2013, a parliamentary standing committee recommended clearer definition of prohibited content expressing concern that the ambiguity could lead to censorship without due process and harassment of intermediaries	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
	Blocked or filtered websites have explanation on why they are blocked or filtered	N	Yes	IT Act Procedure and Safeguards for Blocking for Access of	In 2013, mobile internet access in J&K was suspended for a day after violent protests erupted in the state due to desecrated copy of the Quran by Indian border	Blocking of websites take place under Section 69A of the IT Act. The rules empower the central government to direct any agency or intermediary to block access to	

				Information by Public) "Blocking Rules"	security guards	information when it is satisfied to do, in the interest of "sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence." In certain cases, executive blocking orders are kept confidential and ISP are not legally required to inform the public of blocks and IT law provides no appeal.	
	Content blocking occurs only when ordered by competent judicial authority or independent body	Y	Yes	IT Act Procedure and Safeguards for Blocking for Access of Information by Public) "Blocking	130 court orders to block web content were received by the Information ministry between February 2009 and December 2013.	The blocking rules apply to orders issued by the government agencies. There is an inter-agency process that must be followed under Section 69A of the IT Act where there is a competent independent authority that	

				Rules"		executes the orders.	
	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 production and distribution of content	Y	No	IT Act Procedure and Safeguards for Blocking for Access of Informatio n by Public) "Blocking Rules"	In June 2013, 39 websites has been ordered by the court to be blocked for obscenity	Currently, there is no law in India against viewing pornography. However, both laws prohibit producing and transmitting "obscene material."	
Criminalizing legitimate expressions	Journalists and bloggers are protected against abuse or intimidation	Y	Yes	Article 19 of the Indian Constitutio n IT Act	In August, UP Police detained Kanwal Bharti, scholar, under Section 66A after he posted a Facebook comments in support of a civil servant who allegedly demolished an illegal mosque	The Constitution of India grants citizens the fundamental right to freedom of speech and expression, including the right to gather information and exchange thoughts with others within and outside India. Press freedom is under freedom of expression and speech. However it is subject to restrictions in the interests of state security, friendly	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 country. 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. 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.

						relations with foreign states, public order, decency and morality, contempt of court, defamation, incitement to an offence, and the sovereignty and integrity of India. The Indian Penal Code criminalizes several kinds of speech, including online. Individuals could be punished with jail terms for speech that is found to be seditious, obscene, defamatory, promoting enmity between different groups on grounds of religion, race, place of birth, residence language, prejudicial to maintenance of harmony or consisting statements, rumors, or reports that may cause fear, alarm, disturb public tranquility, or promote enmity or ill will.	

						Individuals can be punished under the Official Secrets Act for wrongful communication of information which may have an adverse effect on sovereignty and integrity of India.	
	Journalists and bloggers are not regularly prosecuted, jailed or fined for libel	U	Yes	Article 19 of the Indian Constitution Article 21 of the Indian Constitution IT Act			Business houses or powerful social groups are more guilty than the state and it is more difficult to hold them accountable.
	Journalists, bloggers and internet users do not engage in self-censorship	N	No				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)
	National security or counter-terrorism laws restrict expression only where: A) the expression is intended to	Y	Yes	Procedure and Safeguards for Blocking for Access of Informatio	According to the Freedom on the Net Report 2014, mobile internet access was suspended and disconnected in Jammu and Kashmir during	Blocking of websites take place under Section 69A of the IT Act. The rules empower the central government to direct any agency or intermediary to	

	incite imminent violence; B) it is likely to incite such violence; and C) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence			n by Public) "Blocking Rules"	2013--due to violence	block access to information when it is satisfied to do, in the interest of "sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence." It also aims to prevent incitement to the commission of any cognizable offence relating the above. In certain cases, executive blocking orders are kept confidential and ISP are not legally required to inform the public of blocks and IT law provides no appeal.	
Imposition of internet intermediary liability	State does not delegate censorship to private entities	N	Yes	Section 79 of the Informatio n Technolog	Mouthshut.com versus Union of India	Section 79 of the IT Act 2008 privatizes censorship	

				y (Amendment) Act, 2008 Section 79A			
	Internet intermediaries are not liable for refusing to take action that infringes on human rights	N	Yes	IT Act 2008 (amendment)	In January 2014, YouTube blocked a video spoofing Rahul Gandhi, citing a copyright claim. Baazi.com judgment	Intermediaries can separately be held liable of infringing the Copyright Act 1957, under the law and licensing agreement. In March 2013, DEITY clarified that intermediaries need to acknowledge complaints within 36 hours and then address them within a month. According to Freedom on the Net report, intermediaries may refuse to remove the content without liability, but are liable to penalties, fines and imprisonment, if the court deems that the information ought to be taken down when challenged in court.	

						Given this framework, intermediaries are incentivized to take down content even in response to illegitimate complaints.	
	State's requests to internet intermediaries to prevent access to content or to disclose private information are: A) strictly limited to purposes such as the administration of criminal justice; and B) by order of a court or independent body	U	Yes	Procedure and Safeguards for Blocking for Access of Information by Public) "Blocking Rules" Intermediary Guidelines 2011	According to Freedom on the Net report, Ministry of Communication and IT told Parliament that 62 URLs were blocked in 2013, citing "hosting objectionable information" with potential to disturb public order. News reports indicate differing numbers of URLs being blocked--some due to violence in the Northeast, particularly violence on September 18th between Hindus and Muslims in the Muzzafarnagar district of UP.	The blocking rules apply to orders issued by the government agencies. There is an inter-agency process that must be followed under Section 69A of the IT Act where there is a competent independent authority that executes the orders. The areas include: sovereignty and integrity of India, defense, security of the state, friendly relations with foreign states or public order or for preventing incitement.	

					Google also received 16 court orders, 147 requests from executive and law enforcement agencies to take down content.		
	There are effective remedies for individuals affected by private corporations' actions, including the possibility of appeal through the procedures provided by the intermediary and competent judicial authority	N	Yes	IT Act implementing guidelines IT Act Rules 2011	On April 29, the Mumbai-based MouthShut.com, a consumer review website, filed a petition to nullify the country's IT Rules (2011). The Supreme Court issued notices to central and state governments in May after the petition was filed. The company sought protection from legal liability for internet intermediaries that host online content. Mouthshut.com and other internet companies received numerous notices from police that demanded either withdrawal of the content or sought the identity of those posting reviews on	Review of implementation guidelines and rules of the IT Act remained pending despite a public statement by the Ministry of Communication and Information Technology in late 2012 that the act would be thoroughly reviewed.	

					their websites.		
	State discloses details of content removal requests and accessibility of websites	N	Yes	IT Act 2000 and 2008 Amendment Procedure and Safeguards for Blocking for Access of Information by Public) "Blocking Rules"	According to the Freedom on the Net report, the Information Ministry received 130 court orders to block web content from February 2009 to December 2013.	Indian courts can order content blocks without the review process. ISPs are not legally required to inform the public of blocks and the IT act provides for no appeal. In fact, Blocking Rules mandate that executive blocking orders be kept confidential.	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.
Disconnecting users from the internet	Internet access is maintained at all times, including during political unrest	N	Yes	IT Act 2000 and 2008 Ammendment Procedure and Safeguards for Blocking for Access of Information by Public) "Blocking Rules"	For example, mobile internet access was suspended on July 18th, 2013 after violent protests erupted in Jammu and Kashmir due to desecrated copy of the Quran at a local religious seminary	In recent times, there have been no incidences of political unrest. However, in times of civil unrest, the government has blocked content and shut down mobile internet access to prevent violence.	
Cyber attacks	State does not carry out cyber	Y	Yes	National Cyber	In India, companies and the	review of implementation	Look at cyber-attacks as Computer Network Exploitation - brought out

	attacks			Security Policy 2013	government have often been victims to cyberattacks. For example, India companies lost around $4 billion due to cyber attacks in 2013 and the amount is set for a 30% jump this year, according to experts. A study ranked India as the fifth-most targeted country globally by phishing attacks. Between July and September 2013, Indian companies suffered a loss of approximately US $53 million via 3,750 attacks. Hackers defaced tens of thousands of websites during the coverage period, a number that has grown five times since 2007	guidelines and rules of the IT Act remained pending despite a public statement by the Ministry of Communication and Information Technology in late 2012 that the act would be thoroughly reviewed.	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. 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. 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
	State takes appropriate and effective measures to investigate actions by third	U	Yes	IT Act 2000 and 2008 Ammend ment		Keeping in view the issue of cyber security, the IT Act 2008 defines "cyber security" and lists	

	parties, holds responsible persons to account, and adopts measures to prevent recurrence					out preventive measures to prevent recurrence	
Protection of the right to privacy and data protection	There are adequate data and privacy protection laws and these apply to the internet	N	No	Article 21 of the Indian Constitution 2011 Rules and IT Act 2000 and 2008 Amendment	On June 26, 2013, Himachal Pradesh anticorruption bureau filed case against unindentified people under sections of the Telegraph and IT Act in relation to surveillance abuse. Incumber Congress government stated that BJP administration tapped over 1,300 phones when the Home Department had authorized 170 taps. These were targeted to political opposition and journalists. There were several allegations of illegal surveillance by the BJP state government of Gujarat in 2009.	The right to privacy is guaranteed under Right to Life under Article 21 of the Indian constitution. Privacy is safeguarded under these laws with respect to multinational companies, but not necessarily, with the government. The Parliamentary Standing Committee recommended clearer definitions of prohibited content, expressing concern that the ambiguity could lead to censorship without due process and harassment of intermediaries Communication surveillance may be	There are adequate data and privacy protection laws and these apply to the internet

					Police, intelligence officials and telecommunications company employees flouted procedure to monitor the communications of an architect from Karnataka for two months. 1996 Judgement of PUCL versus Union of India The E.U. Council on "Committee on legal Affairs and Human Rights". Rajagopal versus Tamil Nadu	conducted under the Telegraph and the IT Act for the following: protect defense, national security, sovereignty, friendly relations with foreign states, public order and to prevent incitement to a cognizable offense. Section 69 A of the IT Act allows surveillance for investigation of any offense. 2011 Rules under the IT Act increased protection of personal data handled by companies, but it does not apply to the government. A privacy bill is in draft stages since 2011 and is subject to discussion within Department of Personnel and Training	
Access	State has a national plan of action for internet access	Y	Yes	National E-Governance Plan aims		According to the 2011 census, 6.3 percent of the total population had	§ Access: The debate in India should be focused on access, because it is a violation of human right if communities lack access to

				to bring public services closer to the citizens National Policy on IT Digital India Program envisioned by Governme nt of India		access to computers or laptops within the household. Half of those with computers or laptops had internet access, and many more citizens had access to the internet through cyber cafes and mobile telephones. According to industry experts, approximately 10 percent of the population had access to the internet. An independent BBC report stated that 121 million citizens were on the internet. According to the Telecom Regulatory Authority of India, 200 million new mobile users subscribed in 2012-13.	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 Net Neutrality: Incorporate Net Neutrality in the checklist as it relates to internet availability, accessibility and affordability
	State fosters independence of new media	Y	Yes	Framewor k & Guidelines for Use of Social Media for Governme	The Union government for the first time conceded before the Supreme Court on Tuesday that it was abuse of power under	Adopting a fresh stance, the government on Wednesday told the Supreme Court that it was willing to take a re-look at Section	

				nt Organisations	Section 66A of Information and Technology Act to arrest two Mumbai-based girls for Facebook posts criticizing shutdown of the city on November 18, 2012 for Shiv Sena chief Bal Thackeray's funeral.	66A of the Information Technology Act, which empowers police to make arrests over social media messages, and to put in necessary safeguards for allaying apprehensions against its misuse. The government assured the court that it was for the complete freedom of expression on the social media and that it was open to framing necessary guidelines to curb misuse of Section 66A and the alleged vagueness in the provision	
	Concrete and effective policy is developed with public and private sector to make the internet available, accessible and affordable to all	Y	Yes	National Policy on IT National Optical Fibre Network (NOFN) National	Intel India has announced plans for delivering digital literacy in the country. The company has announced plans for training persons at the panchayat levels of 1,000 villages that are set	Government's ambitious National Optical Fibre Network (NOFN) aims to provide high-speed broadband connectivity to 2.5 lakh gram panchayats by December 2016 and	

				Digital Literacy Mission	to receive broadband connectivity under the National Optic Fibre Network.	the estimated cost of the project is over Rs 20,100 crore	
	Development programmes and assistance policies facilitate universal internet access	Y	Yes	National E-Governance Plan aims to bring public services closer to the citizens Digital India Initiative National Policy on IT Digital India Program envisioned by Government of India	The government is gearing up for its next big mission, a Rs. 113,000-crore plan that aims to usher in a digital revolution by moving everything online, from education to public services to bureaucracy.		
	State supports production of local multicultural and multilingual content	Y	Yes	Government of India's initiative: Technology Developm	Aptly called 'e-kranti', it comes under the Narendra Modi government's 'Digital India' initiative and is quite simply the	The initiative aims to build the knowledge society online in multiple languagues to reduce language barriers to access of information. For	

				ent for Indian Languages	world's most ambitious broadband project — but one that will have to overcome countless hurdles, big and small. It seeks to provide digital access to all citizens, from the rural and elderly to the poor, according to the government blueprint that HT has viewed	example, low digital literacy and limited knowledge of English impede access. While online content in 17 languages is available, more than 100 languages remain unrepresented.	
	State supports initiatives for meaningful access by marginalised groups	Y	Yes	National E-Governance Plan aims to bring public services closer to the citizens Digital India Initiative National Policy on IT			
	Digital literacy programmes exist, and are easily accessible,	Y	Yes	National E-Governance Plan aims		Number of government sponsored CSCs have increased in	

	including primary school education and training to use the internet safely and securely			to bring public services closer to the citizens Digital India Initiative National Policy on IT		2013. Bangalore, Karnataka becomes the first Indian city to introduce Wi-Fi followed by Patna, Bihar	
International Human Rights Mechanisms and Commitment	State was a signatory to the Human Rights Council Resolution on Freedom of Expression and the Internet	Y	No		No		
	State reports on internet related human rights issues in the UPR		No		No		
	State reports on internet related human rights issues in other treaty body processes		No		No		
Women's Human Rights	State laws uphold women's human rights, including on the internet	Y	Yes				
	State laws prohibit violence against	Y	Yes				

	women online or through the use of information communication technologies and effective remedies are available						
Internet Governance	There are national processes for multi-stakeholder internet governance	Y	Yes				
	State participates in regional and global internet governance forums in a manner that respects, protects and promotes human rights online and offline	Y	No				India is a member of the Multi Stakeholder Advisory Group of the Internet Governance Forum of the United Nations. India's concerns on the issues of public policy on Internet and its Governance is appropriately voiced in the meetings of the IGF through regular participation, holding workshops and Dynamic Coalition meetings and multi-lateral and bi-lateral meetings