India's Universal Periodic Review: Third cycle

Stakeholder Report by the Internet Democracy Project

Internet Democracy Project
A38H, Munirka DDA Flats
New Delhi 110067
India
http://internetdemocracy.in/
contact:
anja@internetdemocracy.in
nayantara@internetdemocracy.in

Status report on
freedom of expression,
freedom of peaceful assembly and association,
right to privacy
in India
as they relate to the Internet

This report is submitted by the Internet Democracy Project, a not-for-profit initiative working for an Internet that supports freedom of expression, democracy and social justice through research, advocacy and debate in India and beyond. It was set up in 2011 as an arm of Point of View, Mumbai. Our priorities and areas of interest in the UPR are freedom of speech and expression, freedom of association and assembly, and the right to privacy in the context of the Internet as well as barriers to Internet access.

Follow up from the Previous Review

1. As Internet rights are a relatively new concern for the Human Rights Council, only Sweden made a relevant recommendation in the previous review, requesting India to ensure 'that measures limiting freedom of expression on the Internet are based on clearly defined criteria in accordance with international human rights standards'.[1]

2. India merely noted this recommendation at the time. The executive or legislative have not taken any steps in the direction of making restrictions to freedom of expression on the Internet conform with international human rights standards since then.

3. However, in *Shreya Singhal v. Union of India*, a landmark judgment in 2015, the Supreme Court of India struck down Section 66A of the Information Technology Amendment Act, 2008, which seeks to punish 'offensive' messages[2], for creating offences that were vague and overbroad, thereby restricting freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India.

4. The Supreme Court also read down Section 79(3)(b) of the IT Act, on intermediary liability, and Rule 3(4) of Information Technology (Intermediary Guidelines) Rules 2011 passed under Section 79, for similar reasons.

Areas of Concern

A. Criminal laws curbing freedom of expression

Content blocking and intimidation under Section 67 of the IT Act

5. Section 67 of the IT Act[3] deals with obscenity. Due to the vague wording of the section, it is frequently used to censor all kind of subject matter – including, but not limited to, sexual content.

6. For example, section 67 has been used to harass and intimidate a journalist working in a remote, conflict-ridden area. Prabhat Singh, a journalist in the Bastar region was arrested under the section (as well as section 292 of the IPC) in March 2016 for sending a Whatsapp message[4], after the police found has message 'offensive'.

7. In June 2016, the section was used by the Department of Electonics and Information Technology (DEITY) to order the blocking of a list of escort websites.[5] This mass blocking is questionable as prostitution is not an offence under the Immoral Traffic Prevention Act, 1956 (ITPA); only soliciting in a public place punishable.[6] Furthermore, section 67 only provides for punishment of obscene content; it does not empower the government to block such websites.

Content blocking under Section 69A of the IT Act

8. The government has powers to block content under Section 69A of the IT Act, for a fairly restricted number of reasons.[7] It has increasingly exercised this power, with a total of 492 URLs blocked under this section in 2015 alone, till November 30th.[8] Only 13 URLs were blocked in 013 and 10 in 2014. Orders passed under this section are secretive and do not lend themselves to scrutiny.

9. Although it is section 69A of the IT Act that explicitly empowers the government to block certain content on the Internet, the government frequently prefers to use section 67 and 79 of the IT Act to justify its blocking orders.

Section 79 of the IT Act

10. In an order dated 31st July 2016, DEITY directed the Department of Telecommunications to notify ISPs to block a list of 857 websites. This was done under Section 79(3)(b) of the IT Act. According to the leaked order that was kept confidential, the blocking was done because 'content hosted on these websites relate to morality, decency given in Article 19(2) of the Constitution'.[9] Under section 69A of the IT Act, this would not have been a valid ground for the government to block content.

11. In April 2016, District Magistrate of Kupwara in Jammu and Kashmir passed an order saying that all group admins of Whatsapp groups have to register themselves in the District Magistrate's office. The Department of Information and Public Relations issued a press release requiring 'proper permission from the concerned Deputy Commissioners' for 'posting news on social media news groups along with sources'. As the court order and the press release make group admins responsible for content shared by members of the group, they turned them into intermediaries under Section 2(w) of the Act. In arrests made, liability under Section 153A of the Indian Penal Code was assigned to Whatsapp group admins, disregarding that section 79(1) of the IT Act protects an intermediary from any liability under any law in force if the intermediary fulfils conditions laid down therein.

Shutdown of Internet services

12. Internet shutdowns in India are imposed[10], not with reference to section 69A of the IT Act and its attendant rules, but through Section 144 of the Criminal Procedure Code. It means that Internet service providers are instructed to suspend 2G, 3G, GPRS, lease line and/or broadband services in the specified regions. No checks and balances to ensure that such shutdowns are indeed legitimate are in place.

13. By September 2016, there have been Internet shutdowns in Jharkhand[11], Jammu & Kashmir[12] and Gujarat[13] this year alone. In 2015, Internet services were shutdown in Nagaland[14], Gujarat, Manipur[15], Kashmir[16], Rajasthan[17]. In 2013 and 2014, Internet services were temporarily banned in Kashmir[18] and Gujarat[19] - sometimes for reasons as frivolous as preventing cheating in an examination.

Criminal defamation

14. In a judgment dellivered in May 2016, the Supreme Court of India upheld the validity of Sections 499 and 500 of the Indian Penal Code, providing for criminal defamation.[20] Currently, a petition in the Supreme Court challenges corporations' claim that its Right to Life can be violated in the context of defamation suits.[21]

15. The criminal defamation provisions have been used to silence the speech on the Internet of a diverse range of actors, including politicians[2223] and media personalities[24], by harassing them with punitive laws that could result in imprisonment upto two years and/or fines in case of conviction.

Sedition

16. Section 124A of the Indian Penal Code deals with sedition. The provision prohibits any signs, visible representations, or words, spoken or written, that can cause 'hatred or contempt, or excite or attempt to excite disaffection' towards the government. As the language of the provision is overly broad, the section has been misused and misapplied to curb freedom of expression and opinion on the Internet, exercised by a large number of people including activists and students.[25]

17. The Supreme Court in multiple cases has read down the provision on sedition, stating clearly, for example, that criticism of the government cannot constitute sedition[26] and requiring an additional condition of incitement to violence[27] or incitement to imminent lawless action[28] to be present to incur liability. Despite such qualifications, multiple cases continue to be booked by law enforcement even where conditions have not been met.[29] The language of the law remains unchanged.

B. Right to Privacy

Lack of legislative protections of the Right to Privacy

18. Although there is no explicit 'right to privacy' in the Constitution of India, the Courts have read this right into Article 21, the right to life and liberty, subject to some restrictions.[30] Moreover, the Courts have also ruled that the right may be curtailed only through procedure established by law, where the procedure is fair, just and reasonable.[31] Legislative guidance on this issue remains, however, absent.

19. This interpretation of the right to privacy under Article 21 has now been challenged, however, by the government in a writ petition.[32] The Attorney General of India argued in the Supreme Court that the right to privacy cannot be read into the Indian constitution.[33]

Expanding surveillance in the name of intelligence gathering

20. The Indian State's surveillance powers are expanding, and several new intelligence gathering bodies have been formed in the last four years,[34] leading to increasing citizen data collection in the name of eliminating threats to national security, without concomitant privacy protections.

21. There is also no statutory redressal mechanism in case of illegal interception and monitoring of information and communications by the State or private parties.

22. Intelligence agencies are exempt from disclosing information about themselves under section 11 of the Right To Information Act 2005 and operate without judicial or legislative oversight. In addition, the intelligence community has been pushing for exemption under privacy bills that have been under deliberation.

23. Surveillance mechanisms such as the Central Monitoring System[35] and the National Intelligence Grid (NATGRID)[36] arguably do not conform with any of the 'International Principles on the Application of Human Rights to Communications Surveillance'. [37]

Encryption

24. The permitted upper limit for encryption strength in India is 40 bits in symmetric algorithms, for ISPs and individuals alike,[38] an extremely weak standard.

25. Under Section 84 of the IT Act, the government released a draft encryption policy[39] in September 2015, which required (a) all application service providers to deposit private keys to help law enforcement and other authorised parties to access the contents of the communication (b) users to store plain text of their messages upto 90 days. This policy endangered the privacy of users and defied the very utility of encryption by asking users to store information insecurely.This was rolled back after severe public pressure. A new draft of the encryption policy was released selectively only to the private sector in 2016.

Aadhaar Bill

26. While the Aadhaar Act, 2016, purports to ensure the use of India's Unique Identification scheme to make government delivery of welfare schemes more efficient, it also empowers the Unique Identity Authority of India (UIDAI) to disclose many fields of information upon a simple authentication request by government agencies and private actors. Without a privacy legislation that contains redressal mechanisms, this identity number attached to demographic and biometric information is liable to be misused.

C. Reducing barriers to access

Restrictions on access to mobile phones for women and girls

27. *Khap panchayats* (local community bodies) in villages of Uttar Pradesh,[40] Rajasthan[41] and Gujarat[42] have imposed a ban on the usage of social media and mobile phones for women in the areas, especially young and unmarried women. The lack of disavowal of and strong action against *khap panchayats* who are banning the use of mobile phones among women, is disconcerting.

Recommendations

A. Criminal laws curbing freedom of expression

30. Amend the rules under Section 69A of the IT Act to remove secrecy of the orders.

31. Ensure blocking orders by the government are passed only under Section 69A of the IT Act, and the reasons fall strictly within the limits provided in the section. Require court orders for all other blocking orders.

32. Bring an immediate end to the use of section 144 IPC to justify network shutdowns in the name of law and order.

33. Amend the Indian Penal Code to strike down provisions on criminal defamation, in compliance with international human rights standards. The aggrieved party is still free to pursue civil remedy.

34. Amend the Indian Penal Code provisions on sedition in line with the Supreme Court's guidelines.

B. Right to Privacy

35. Pass a law providing strong protections of the right to privacy

36. Proscribe clear limits on government surveillance and discontinue bulk collection of citizen data, in compliance with international human rights standards

37. Comply with the order passed by the Courts to not make Aadhaar mandatory for delivery of welfare services. Prohibit UIDAI from disclosing biometric or demographic information to government bodies or private bodies. Place strong penalties and create redressal mechanisms for breach of data either by sub-contractors or government agencies.

38. Require the use of strong encryption in business and government communications as well as individual communications. The government should not require manufacturers of software and hardware to insert backdoors, or deposit private keys with the government, creating security vulnerabilities.

C. Reducing barriers to access

39. Take strong measures against and issue guidelines for community bodies imposing restrictions on the use of mobile phones by women.

---

1 See (UPR 2- 138.126)

2 66-A. 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; or

(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 suchmessages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.— For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

3 Section 67. 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.

4 http://www.newslaundry.com/2016/08/02/nl-interviews-with-prabhat-singh-reporting-from-the-media-black-hole-of-bastar/.

5 http://www.catchnews.com/national-news/dot-order-banning-857-porn-websites-in-name-morality-and-decency-1438593006.html.

6 Section 8: Seducing or soliciting for purpose of prostitution.—Whoever, in any public place or within sight of, and in such manner as to be seen or heard from, any public place, whether from within any building or house or not—

(a) by words, gestures, wilful exposure of his person (whether by sitting by a window or on the balcony of a building or house or in any other way), or otherwise tempts or endeavours to tempt, or attracts or endeavours to attract the attention of, any person for the purpose of prostitution; or

(b) solicits or molests any person, or loiters or acts in such manner as to cause obstruction or annoyance to persons residing nearby or passing by such public place or to offend against public decency, for the purpose of prostitution, shall be punishable on first conviction with imprisonment for a term which may extend to six months, or with fine which may extend to five hundred rupees, or with both, and in the event of a second or subsequent conviction, with imprisonment

for a term which may extend to one year, and also with fine which may extend to five hundred rupees: [Provided that where an offence under this section is committed by a man, he shall be punishable with imprisonment for a period of not less than seven days but which may extend to three months.]

[7] These are: 'in the interest of the sovereignty and integrity of India, defence 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.'

[8] http://indianexpress.com/article/technology/tech-news-technology/492-social-media-urls-blocked-in-2015-under-sec-69a-only-10-in-2014/.

[9] http://cis-india.org/internet-governance/resources/dot-morality-block-order-2015-07-31/view.

[10]

[11] http://www.medianama.com/2016/04/223-mobile-internet-ban-gujarat-bokaro/.

[12] http://www.hindustantimes.com/india/handwara-firing-mobile-internet-services-suspended-in-kashmir/story-iPQHs3vdmiWx7w0uCGK8NJ.html.

[13] http://www.medianama.com/2016/04/223-mobile-internet-ban-gujarat-bokaro/.

[14] http://www.huffingtonpost.in/2015/03/09/nagaland-lynching_n_6828442.html.

[15] http://scroll.in/article/753108/why-a-blanket-ban-on-the-internet-in-troubled-manipur-is-not-a-good-idea.

[16] http://www.medianama.com/2015/09/223-jammu-and-kashmir-internet-ban/.

[17] http://www.medianama.com/2015/12/223-rajasthan-internet-block/.

[18] http://timesofindia.indiatimes.com/india/Afzal-Guru-hanged-Mobile-internet-services-snapped-in-Kashmir/articleshow/18415453.cms.

[19] http://sflc.in/legality-of-internet-shutdowns-under-section-144-crpc/.

[20] See *Subramanian Swamy and others vs. Union of India*.

[21] http://indianexpress.com/article/india/india-news-india/supreme-court-to-examine-if-firms-can-file-libel-cases-greenpeace-essar-power-company-3015596/.

[22] http://indiatoday.intoday.in/story/arvind-kejriwal-notice-twitterati-slams-back/1/760331.html.

[23] http://indiatoday.intoday.in/story/subramanian-swamy-j-jayalalithaa-defamation-case-twitter-comment/1/384550.html.

[24] http://www.dnaindia.com/entertainment/report-krk-responds-to-defamation-case-filed-against-him-by-vikram-bhatt-2227514.

[25] Most recently, a person liking a political cartoon on Facebook was charged under the section in Durg, Chhattisgarh, and since has been denied bail twice by the sessions court. See http://www.thehoot.org/media-watch/digital-media/why-is-tauseef-bhat-in-jail-9616. For another example, see http://indiatoday.intoday.in/story/kerala-man-arrested-for-derogatory-comment-about-pathankot-martyr-lt-col-niranjan-kumar/1/562791.html

[26] http://thewire.in/64281/criticism-of-government-does-not-constitute-sedition-says-supreme-court/.

[27] See *Kedar Nath v. State of Bihar*.

[28] See *Indra Das v. State of Assam.*

[29] http://thewire.in/10336/its-time-to-put-an-end-to-maharashtras-love-affair-with-the-law-of-sedition/.

[30] In *Govind* v. *State of M.P* 1975 AIR 1378, the Court ruled that the right may be restricted if there is an important countervailing interest which is superior, if there is a compelling state interest to be served, in the interests of the general public or for the protection of the interests of Scheduled Tribes.

[31] *Maneka Gandhi* v. *Union of India* (1978) 2 SCR 621.

[32] *Justice K.S Puttaswamy & Another vs. Union of India and Others* (2014) 6 SCC 433.

[33] http://articles.economictimes.indiatimes.com/2015-07-23/news/64773078_1_fundamental-right-attorney-general-mukul-rohatgi-privacy.

[34] For example, NATGRID, National Counter Terrorism Centre, National Cyber Coordination Centre, New Media Wing.

[35] The Central Monitoring System is a telecommunications interception system that enables agencies of the government to intercept communications without requiring to liaise with the telecom service providers. For more, see e.g. http://scroll.in/article/729701/congress-minister-who-put-surveillance-system-in-place-warns-against-its-lawful-but-malicious-use.

[36] NATGRID centralises 21 databases, including information from banks, credit card, Internet, cell phones, immigration, motor vehicle departments, railways, National Crime Records Bureau, Securities and Exchange Board of India and Income Tax Department, with the aim of giving a full profile of persons to security agencies that seek it.

[37] https://necessaryandproportionate.org/principles.

[38] As per the License Agreement that Internet Service Provider (ISP) licensees have to enter into.

[39] https://cdn.netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf.

[40] http://timesofindia.indiatimes.com/city/agra/Panchayat-bans-mobile-phones-among-girls/articleshow/51060339.cms, http://www.thehindu.com/news/national/other-states/uttar-pradesh-community-panchayat-bans-jeans-mobile-phones-for-girls/article6298539.ece.

[41] http://zeenews.india.com/news/rajasthan/khap-panchayat-strikes-again-mobile-phones-use-banned-for-girls-in-barmer_1623430.html.

[42] http://www.hindustantimes.com/india/gujarat-village-bans-mobile-phones-for-unmarried-women/story-iziKwjYckgmOOP8ZRBNn3K.html.