

COALITION SUBMISSION TO THE UNIVERSAL PERIODIC REVIEW OF INDIA

INTERNET RIGHTS, FREEDOM OF EXPRESSION (FOE) ONLINE AND
FREEDOM OF ASSOCIATION AND ASSEMBLY (FOAA) ONLINE IN INDIA

For Consideration at the 27th Session UN Working Group in 2017
22 September 2016

Digital Empowerment Foundation (DEF) | Internet Democracy Project (IDP)
Point of View (PoV) | Nazdeek | Association for Progressive Communications (APC)

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.



COALITION SUBMISSION TO THE UNIVERSAL PERIODIC REVIEW OF INDIA

INTERNET RIGHTS, FREEDOM OF EXPRESSION (FOE) ONLINE AND
FREEDOM OF ASSOCIATION AND ASSEMBLY (FOAA) ONLINE IN INDIA

For Consideration at the 27th Session UN Working Group in 2017
22 September 2016

Digital Empowerment Foundation (DEF) | Internet Democracy Project (IDP)
Point of View (PoV) | Nazdeek | Association for Progressive Communications (APC)



CONTENT

INTRODUCTION	7
Executive Summary	9
Access to Internet	11
Right to Information	13
Freedom of Opinion and Expression Online	16
Right to Privacy	20
Freedom of Association and Assembly Online	23
Gender and the Internet	26
Cyber Crime and Sexual exploitation	29
International Mechanisms	30
Recommendations to the GoI	31

INTRODUCTION

- 1. Digital Empowerment Foundation (DEF)** works with underdeveloped and marginalised communities and people living in socio-economically backward conditions by empowering them through technology. It advocates for the protection and promotion of human rights on the internet. The internet can be an effective tool for social change and development and thus DEF works towards promoting freedom of expression, assembly, association, privacy, right to information and access on the internet.
- 2. The Internet Democracy Project** advocates for freedom of expression, democracy and social justice, in India and beyond. The Internet Democracy Project does research and advocacy on issues of freedom of expression, cybersecurity, surveillance and human rights on the Internet. It has also been actively involved in Internet governance mechanisms at the ITU¹, in the WSIS² and regional and global Internet Governance Forums, and in national consultations on emerging policy issues like network neutrality regulations.
- 3. Point of View (POV)** aims to amplify the voices of women and remove barriers to free speech and expression by using a variety of media, art and culture platforms, both offline and online. It is involved in research, debate and discussion, and advocacy on the issues of gender, sexuality, freedom of expression and sexual expression, sexuality and disability, digital rights at the intersection of gender, sexuality and technology. POV has been part of various national, regional and international forums on the internet, technology, disability etc., striving to bring in the gender and sexuality perspective.
- 4. Nazdeek** is a legal-capacity building organisation dedicated to bringing access to justice closer to marginalised communities in India. Our model fuses grassroots legal education, community monitoring of service delivery, use of judicial and non-judicial remedies, and strategic research and advocacy to advance socio-economic rights with a focus on maternal health, nutrition, housing and labor in Delhi and Assam.

1 International Telecommunications Union (ITU); <https://www.itu.int>

2 World Summit on the Information Society (WSIS); <http://www.itu.int/net/wsisis/>

-
5. **Association for Progressive Communications (APC)** is a network of organisations across the world, primarily advocating for the protection, promotion and respect of human rights on the internet. APC aims to empower and support organisations, social movements and individuals in and through the use of ICTs, to build strategic communities and initiatives for the purpose of making meaningful contributions to equitable human development, social justice, participatory political processes and environmental sustainability. It is actively engaged in internet governance mechanisms and processes at the WSIS, UNHRC³ and the regional and international internet governance forums.
6. Given the significance of the internet in the lives of people and their areas of expertise of these organisations, this submission presents an overview of the status of the exercise of human rights on the Internet in India, including with regard to access to information, privacy, surveillance and monitoring in the name of intelligence gathering, attempts to weaken encryption, network shutdowns and other communication services; and restrictions on women's access to technology and the internet. 7. Access to the internet empowers us to exercise various human rights i.e. civil and political rights as well as economic, social and cultural rights. While the Government of India (GoI) has initiated programmes like the Digital India Initiative and National Optical Fibre Network (NOFN), there is a substantial gap between policy, programmes and the on ground reality.

.....

3 United Nations Human Rights Council (UNHRC); <http://www.ohchr.org/en/hrbodies/hrc/pages/hrcindex.aspx>

EXECUTIVE SUMMARY

7. Access to the internet empowers us to exercise various human rights i.e. civil and political rights as well as economic, social and cultural rights. While the Government of India (GoI) has initiated programmes like the Digital India⁴ Initiative and National Optical Fibre Network (NOFN)⁵, there is a substantial gap between policy, programmes and the on ground reality.
8. In the second cycle of the Universal Periodic Review (UPR), in 2012, India had received two recommendations relevant to the topics covered in this submission: one recommendation on taking measures to ensure that any restrictions on the right to freedom of expression on the internet are in line with international standards and obligations (no.126) and one recommendation on ensuring a safe environment for journalists (no. 127). While the recommendation on safety of journalists was accepted in revised form, the recommendation on restrictions on the internet was not accepted by the GoI⁶. In the last four years, the GoI has made little to no progress in improving the exercise of human rights on the internet or facilitated by the internet. Reprisals against free speech and dissent continue while perpetrators, both state and non-state, enjoy impunity.
9. Since the previous review, there has been increase in number of state-led crackdowns on freedom of expression (FoE) and speech on the internet. The nature of attacks ranges from censorship of URL/websites and network shutdowns to arrests of citizens for engaging in online activities to form associations; especially on social media platforms and digital communication applications such as Twitter, Facebook and WhatsApp.
10. Reported cases indicate a lack of transparency and non-compliance with procedures established by national law and international standards when it comes to blocking and censorship. Often times state action against FOE is triggered based on arguments relating to upholding moral and religious standards. Extensive use of national

4 Digital India is flagship initiative of Government of India with a vision to transform India into a digitally empowered society and knowledge economy; <http://digitalindia.gov.in/content/about-programme>

5 The National Optical Fibre Network (NOFN) is a project initiated in 2011 and funded by Universal Service Obligation Fund (USOF) to provide broadband connectivity to 250,00 Village Councils; <http://www.bbnl.nic.in/index1.aspx?lsid=249&lev=2&lid=21&langid=1>

6 Report of the Working Group on the Universal Periodic Review: India, 2012, A/HRC/21/10, available at: <http://daccessdds-ny.un.org/doc/UNDOC/GEN/G12/151/08/PDF/G1215108.pdf?OpenElement>

legislation including the sedition law (section 124A of the IPC) to curtail FOE, FOAA, and regressive provisions such as Sections 66A, 67, 67A, 69, 69A and 69B of the Information and Technology Act, 2000 (IT Act) against FOE has been on the rise.

11. New laws and policies with provisions that curtail human rights have been under deliberations such as the Privacy Bill, 2013; Draft National Encryption Policy, 2015, and DNA Profiling Bill, 2015 are extending more powers to the state, especially intelligence agencies to encourage surveillance and intercept and monitor communications with little to no redressal mechanism.
12. Women face greater barriers in accessing ICTs because of the existing socio-economic structural inequalities. Worryingly, it is noted that, increasingly, local governance bodies are barring women from using mobile phones and internet in rural areas. Non-consensual circulation of films recorded during consensual and non-consensual sexual acts, to blackmail and silence women and prevents them from seeking redressal in cases of rape, is on the rise. These 'rape videos' are treated as 'obscene' material instead of being treated as a violation of consent.

ACCESS TO INTERNET

13. Access to the internet is the basic necessity which would enable the exercise of a whole host of other rights in online spaces. This particularly includes our right to access and disseminate information. The Gol launched the Digital India Initiative in 2015 with vision of empowering the country digitally. During the launch event, the Gol recognised digital access as human right⁷. Additionally, NOFN plan was initiated in 2012, to provide high-speed broadband connectivity to 250,000 village councils by December 2016, by laying 700,000 km of optical fibre cable by that time. The National Telecom Policy (NTP), 2012 also notes that telecom and broadband connectivity are basic necessities like education and health, and encourages working towards 'Right to Broadband'⁸. Despite these developments, the implementation of these initiatives is substandard- the cables are yet to be laid in the pipes and servers are not available at the access points⁹. In a country that envisions becoming a digital superpower and is currently one of the largest exporters of Information Technology and Information Technology Enabled Services (IT & ITeS), only 19% of the population has access to the internet¹⁰.

a. Access for People with Disabilities

14. According to the Census of India 2011, approximately 27 million people in India are disabled, or 2.21 % of the total population¹¹. There is no existing specific legislation in India that ensures access to ICTs for persons with disabilities.
15. In 2011, the Department of Telecommunications (DOT¹²), under the Ministry of Communications and IT, launched a pilot project to provide access to ICTs and ICT-enabled services for persons with disabilities in rural India, facilitated by USOF¹³.

7 Digital India Programme, Government of India, <http://www.digitalindia.gov.in/content/about-programme>

8 National Telecom Policy 2012, Telecom Regulatory Authority of India, available at:<http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final.pdf>

9 "For 800 million citizens, Modi's Digital India highway is a bridge to nowhere", Scroll.in, May 26, 2016, available at: <http://scroll.in/article/808622/for-800-million-citizens-modis-digital-india-highway-is-a-bridge-to-nowhere>

10 Internet users data, internet live stats, available at: <http://www.internetlivestats.com/internet-users/>

11 Census of India 2011, Disability data; <http://www.disabilityaffairs.gov.in/upload/uploadfiles/files/disabilityinindia2011data.pdf>

12 Department of Telecommunications; <http://www.dot.gov.in>

13 Concept Paper July 2011, Access to ICTs and ICT Enabled Services for Persons with Disabilities in Rural India, Pilot Project Scheme, Ministry of Communications & IT

However, there has been no report on the status of the implementation of the project by DOT since then.

16. The government has not fully adopted universal design mechanisms prescribed in the Web Content Accessibility Guidelines 2.0 (WCAG) of the World Wide Web Consortium (W3C¹⁴). The absence of universal design renders assistive technologies ineffective due to incompatibility with internet standards. This in turn contributes to increased digital exclusion for persons with disabilities (PWDs).

Department of Telecommunications, Universal Service Obligation Fund, available at http://usof.gov.in/usof-cms/miscellaneous/Concept%20paper_USOF%20Scheme_PwDs_A.G.Gulati.pdf

14 W3C guidelines, World Wide Web Consortium, available at: <https://www.w3.org/standards/webdesign/accessibility>

RIGHT TO INFORMATION

a. Right to Information Act 2005

17. The Right to Information Act 2005 (RTI) enables us to seek information, demand transparency and hold the government accountable. There is also a provision for filing RTI requests online. In 2006, the GoI formulated the Common Service Centre (CSC) programme under the National e-Governance Plan (NeGP) as a Mission Mode Project (MMP), and as of January 2011, only 87,000 CSCs of the 236,000 planned have been established. Given that the internet penetration in rural India stands at only 9%¹⁵, these CSCs can be effectively used as public internet access points for citizens who seek assistance and redressal for filing RTIs online.
18. According to the Central Information Commission's (CIC) annual report 2014-2015¹⁶, the rejection rate of applications during this period was 8.4 %, the highest in eight years. Even applications that are not 'sensitive' in nature are rejected. The rejection rates reported from the Office of the Prime Minister, Ministry of Home Ministry and the Ministry of Finance are 22%, 16% and 20.2% respectively¹⁷.
19. Another worrying trend relates to the increase in the number of attacks on journalists and HRDs who use the RTI in their work. Since 2005, at least 45 RTI activists have been killed¹⁸; of the 289 reported attacks on activists, the maximum number of killings has been recorded from Maharashtra¹⁹.
20. Section 4 of the RTI Act mandates all public authorities to disclose information suo-moto in their annual reports. However, only 75.27 % of public departments have filed their annual reports, which include suo-moto disclosures, according to the CIC

15 "Only 9% of rural India has access to mobile internet: Report", Times of India, Feb. 3, 2016 (<http://timesofindia.indiatimes.com/tech/tech-news/Only-9-of-rural-India-has-access-to-mobile-internet-Report/articleshow/50840296.cms>)

16 Annual Report 2014 – 2015, Central Information Commission, available at: <http://cic.gov.in/AnnualReports/AR-2014-15/AR2014-15E.pdf>

17 Under Modi rule, RTI rejection rate goes up; Report by Governance Now <http://www.governancenow.com/news/regular-story/-modi-rule-rti-rejection-rate-goes-up>

18 India: New Killing of 'Right-to-Information' Activist, Human Rights Watch, Sep. 10, 2015, <https://www.hrw.org/news/2015/09/10/india-new-killing-right-information-activist>

19 Most RTI activists killed in Maharashtra since law came about; Gujarat, UP come second", Firstpost, Sep. 7, 2015 (<http://www.firstpost.com/india/most-rti-activists-killed-in-maharashtra-since-law-came-about-gujarat-up-come-second-2424162.html>)

report 2014-2015²⁰. As a curative measure, the GoI issued an order on 29 June 2015 to ensure compliance for effective implementation of section 4 by all public authorities. Another official memorandum was passed on July 9 2015, for appointing nodal officers to monitor section 4's implementation²¹. If these disclosures are made periodically on websites of the respective departments, the burden on the staff as well as the citizens would considerably reduce and thus contribute to better governance and transparency.

b Open Government Data (OGD)

21. In 2012, the GoI launched an online portal (data.gov.in) to make information available to the public about all government departments. The available information ranges from public transport routes to electoral candidate records and municipal body phone numbers. This initiative made promises of greater transparency and accountability as envisioned by section 4(2) of the RTI Act as well as addressing the shortcomings of the RTI Act.
22. The government's efforts and long-term commitment towards making data voluntarily available to the public, for access to information and accountability, is appreciable, with over 18,000 datasets²² that have been uploaded so far. However, there are various challenges that hinder the achievement of these goals, not only for the government but also citizens, researchers, civil society, media, academia and HRDs. The Department of Science and Technology (DST) policy guidelines, the National Data Sharing and Accessibility Policy (NDSAP) are incomprehensible²³. Therefore, the data that is being shared by government agencies is often not relevant. As a result, the available data is out-dated, incomplete, duplicated, inadequately referenced and lacks critical properties as well as metadata (for e.g. sources and references²⁴).

20 Annual Report 2014 – 2015, Central Information Commission, available at: <http://cic.gov.in/AnnualReports/AR-2014-15/AR2014-15E.pdf>

21 "Only 75.27 per cent departments following mandatory RTI clause", India Today, April 28, 2016 (<http://indiatoday.intoday.in/story/only-75-27-per-cent-departments-following-mandatory-rti-clause/1/653885.html>)

22 "India must do more to see impact of open data", Web Foundation, Nov. 16, 2015 (<http://webfoundation.org/2015/11/india-must-do-more-to-see-impact-of-open-data/>)

23 "India must do more to see impact of open data", Web Foundation, Nov. 16, 2015, available at: <http://webfoundation.org/2015/11/india-must-do-more-to-see-impact-of-open-data/>

24 "Building the data economy in India", Live Mint, Ja. 8, 2015, available at: <http://www.livemint.com/Opinion/p1hm2br46sFPMYp39Zn1eN/Building-the-data-economy-in-India.html>

-
23. In addition, the processes required to effectively operationalise such platforms are inadequate. A lack of coordination within government departments, an inability to judge effectively what data would be useful to upload and the complete absence of some government agencies and departments from portal leave little to no room for data analyses and data comparison. These shortcomings make difficult to use the datasets and portal in a substantive manner, making them more or less redundant.

FREEDOM OF OPINION AND EXPRESSION ONLINE

24. The internet has opened up many opportunities for citizens and groups to exercise their right to freedom of expression and opinion, which was otherwise restricted in access to a few, on traditional platforms. Perhaps, the most significant civil rights exercised on the internet is the right to freedom of expression and opinion, which is also an enabler for the enforcement of other rights. Unfortunately, we note that this is also the right that is most under threat of violation on the internet.
25. In June 2014, a 24-year old IT professional was killed in Pune, by a mob of Hindu Rashtra Sena (a radical Hindu outfit) members for uploading alleged derogatory pictures of Hindu gods and Balasaheb Thakrey, chief of Shiv Sena²⁵. In January 2012, political cartoonist, Mr Aseem Trivedi²⁶ was arrested on sedition charges and his website was blocked for publishing a cartoon on corruption in the country. In an instance of censorship through intermediaries, in May 2012, Google²⁷ was asked to remove a blog for containing allegedly 'defamatory' content on a spiritual leader by the Delhi High Court, citing section 69A of the IT act (Power to issue directions for blocking public access of any information through any computer). Towards the end of 2012, Mr Ravi Srinivasan, arrested under 66A of the IT Act²⁸ became the first person ever in India to be arrested for posting a tweet²⁹. These cases are few among the many that pile on every day and is indicative of the severely restrictive environment in which this right is exercised online in India

a. Use of criminal law to stifle free speech online

26. In addition to specific cyber and technology laws like the IT Act, provisions in traditional penal laws such as hate speech, criminal defamation and sedition in the

25 "Muslim techie beaten to death in Pune, 7 men of Hindu outfit held", Indian Express, June 4, 2014 (<http://indianexpress.com/article/india/politics/muslim-techie-beaten-to-death-in-pune-7-men-of-hindu-outfit-held/>)

26 "Indian cartoonist Aseem Trivedi jailed after arrest on sedition charges" The Guardian, Sep. 10, 2012 (<http://www.theguardian.com/world/2012/sep/10/indian-cartoonist-jailed-sedition>)

27 "Delhi High Court Directs Google To Remove Defamatory Content Against Sri Sri Ravi Shankar" Medianama, May 11, 2012 (<http://www.medianama.com/2012/05/223-delhi-high-court-directs-google-to-remove-defamatory-content-against-sri-sri-ravi-shankar/>)

28 The Section 66A defines the punishment for sending "offensive" messages through a computer or any other communication device like a mobile phone or a tablet. A conviction can fetch a maximum of three years in jail and a fine

29 "Why was an Indian man held for sending a tweet?" BBC, Nov. 6, 2012 (<http://www.bbc.com/news/world-asia-india-20202275>)

Indian Penal Code (IPC) are used by authorities disproportionately and arbitrarily to shut down dissent and criminalise expression. This trend has unfortunately spiked considerably since the last review. In November 2012, Shaheen Dhada and Rinu Srinivasan from Maharashtra were arrested under section 66A of the IT Act and section 295A (criminalises engendering religious hate speech) of the IPC, among other charges, for putting up a Facebook post³⁰. However, on a positive note, the Supreme Court of India took a progressive position in relation to the vague and repressive language of section 66A of the IT Act, striking it down in 2015 as being violative of fundamental rights in the Constitution of India. In doing so, the Supreme Court made specific observations on the importance of upholding the right to freedom of expression and dissent on the internet³¹. However, there is evidence that shows that the police have filed cases under Section 66A even after the courts striking down³².

27. While the overall environment for FOE online is restrictive as demonstrated above, the situation for women poses an additional and dangerous challenge. Several instances of sexual hate speech and incitement of sexual violence against women online have been noted on account of their exercise of FOE on political, social and religious issues. One such instance was recorded in May 2016 against a feminist activist Ms. Kavita Krishnan who was subjected to harassment and intimidation online for her opinions³³. Similarly, in August 2016 Divya Spandana (screen name Ramya), an actor and politician was harassed online for her comments against hatred towards a neighbouring country. A sedition case has also been filed against Ms. Spandana³⁴.
28. Political speech and religion related speech online remain the most targeted. Instead

30 "India Facebook arrests: Shaheen and Renu speak out" BBC, Nov. 26, 2012 (<http://www.bbc.com/news/world-asia-india-20490823>)

31 Supreme Court of India, Shreya Singhal Vs Union of India, Writ Petition (Criminal) No. 167 of 2016, available at: http://supremecourtindia.nic.in/FileServer/2015-03-24_1427183283.pdf

32 <http://www.hindustantimes.com/india-news/despite-sc-order-thousands-booked-under-scrapped-section-66a-of-it-act/story-DisRxFDBJTXvkz6ZW4fRHK.html>

33 "Of course I had free sex: How feminist Kavita Krishnan's mom silenced a troll on Facebook", Indian Express, May 16, 2016 (<http://indianexpress.com/article/trending/trending-in-india/of-course-i-had-free-sex-how-feminist-kavita-krishnans-mom-shut-up-a-troll-on-facebook-2803195/>)

34 "Kannada actor-politician Ramya faces sedition charges for pro Pakistan comments", Firstpost, Aug. 23 2016 (<http://www.firstpost.com/bollywood/kannada-actor-politician-ramya-faces-sedition-charges-pro-pakistan-comments-2971520.html>)

of condemning such acts, several instances are propagated by elected politicians³⁵ and ministers³⁶ perpetrating hate speech against minorities. The Supreme Court has intervened in some of the cases³⁷.

b. Blocking

29. In 2012, to control rumour and fear mongering around violence against people from North-East India living in Bangalore, the DOT had blocked over 200 webpages, which were alleged to have contained inflammatory content. In addition, social networking websites³⁸ were directed to remove inflammatory content that could incite communal violence. These blocks are inordinate and undemocratic knee jerk reactions that don't solve the purpose there is no defined criteria as to what counts as inflammatory.
30. In April 2013, in an instance of censorship through intermediaries, the website of an international NGO, CARE was blocked in India, observed from at least two Internet Service Providers (ISPs)³⁹. The government's ban on 39 pornographic websites including image sharing and hosting platforms in July 2013 reaffirmed the lack of procedures and transparency. Many of these websites were not even pornographic websites⁴⁰. 32 websites were blocked in November 2014 on the suspicion of promoting jihadist propaganda⁴¹.
31. According to a report, launched in December 2015 on content blocking by Facebook,

35 "In Dadri, BJP legislator Sangeet Som warns: 'Befitting reply if innocents framed'", Indian Express, Oct. 5, 2015 (<http://indianexpress.com/article/india/india-news-india/in-dadri-sangeet-som-accuses-up-govt-of-framing-innocent-for-lynching-incident/>)

36 "Dalit Children Deaths: Union Minister VK Singh's 'Dog' Remark Sparks Controversy", NDTV Online, Oct 22, 2015 (<http://www.ndtv.com/india-news/not-governments-fault-if-one-stones-a-dog-vk-singh-on-dalit-childrens-killings-1235137>)

37 "Hate speech: Supreme Court names Raj Thackeray, Owaisi, Togadia", Indian Express, April 9, 2013 (<http://indianexpress.com/article/news-archive/web/hate-speech-supreme-court-names-raj-thackeray-owaisi-togadia/>)

38 "India targets social media sites after Assam violence", BBC, Aug. 22, 2012 (<http://www.bbc.com/news/technology-19343887>)

39 "Why Is Care.org Blocked On Vodafone & Spectranet?", Medianama, April 9, 2013 (<http://www.medianama.com/2013/04/223-why-is-care-org-blocked-on-vodafone-spectranet/>)

40 "Govt goes after porn, makes ISPs ban sites" The Times of India, June 26, 2013 (<http://timesofindia.indiatimes.com/tech/tech-news/Govt-goes-after-porn-makes-ISPs-ban-sites/articleshow/20769326.cms>)

41 "A threat from ISIL prompted India to block Github and 31 other sites" Quartz India, Dec. 31, 2014 (<http://qz.com/319866/a-threat-from-isis-prompts-india-to-block-github-and-a-handful-of-other-sites/>)

India was named one of the top countries to request content blocking from the social networking site. The reported requests were received from law enforcement agencies⁴². Google also reports a similar trend with over 1600 item removal requests from June to December 2015⁴³.

32. In an attempt to curtail freedom of sexual expression in the name of protecting morality and culture, the DOT had blocked 240 websites providing escort services in June 2016⁴⁴. This is as illegal as buying or selling of sex per se is not criminalised under the Immoral Traffic (Prevention) Act, 1956.
33. This increase in instances of websites blocking is clearly indicative of the heightening of censorship of online spaces. Oftentimes, such blocking is done in an arbitrary manner without following due process.

42 "India tops list of requests for blocking content on Facebook" Indian Express, April 13, 2014 (<http://indianexpress.com/article/lifestyle/life-style/india-tops-list-of-requests-for-blocking-content-on-facebook/>)

43 <https://www.google.com/transparencyreport/removals/government/IN/>

44 "Ban on online escort services is an assault on freedom. Here's why", Catch News, June 15, 2016 (<http://www.catchnews.com/culture-news/ban-on-online-escort-services-is-an-assault-on-freedom-here-s-why-1465995228.html/fullview>)

RIGHT TO PRIVACY

a. Surveillance

34. Domestically, the number of intelligence agencies are increasing, and their powers are exercised without judicial or legislative oversight. Several new intelligence gathering bodies have been formed⁴⁵ in the last 4 years, leading to increasing citizen data collection in the name of improving governance and eliminating threats to national security, without concomitant privacy protections.
35. India's mass surveillance architecture includes the Central Monitoring System (CMS), a telecommunications interception system that enables agencies of the government to intercept communications without requiring to liaise with the telecom service providers⁴⁶.
36. The National Intelligence Grid (NATGRID) centralises 21 databases giving full profile of suspects, to security agencies who seek it. No information about the checks and balances are available. Such liberal intelligence sharing is in conflict with principles of necessity and proportionality⁴⁷.

b. Privacy

37. The Right to Privacy has been enshrined as a fundamental human right in various international instruments, which India is a signatory to⁴⁸. While there is no explicit recognition of the right to privacy in the Constitution of India, an examination of jurisprudence over the years shows that right to privacy has been read into Article 21 (right to life) by Indian Courts⁴⁹. However, this interpretation has now been challenged by the government in a writ petition, Justice K.S Puttaswamy & Another vs. Union of India and Others, with the Attorney General of India arguing in the Supreme Court that

45 NATGRID, National Counter Terrorism Centre, National Cyber Coordination Centre, New Media Wing

46 Congress minister who put surveillance system in place warns against its 'lawful but malicious' use" Scroll, May 28, 2015 (<http://scroll.in/article/729701/congress-minister-who-put-surveillance-system-in-place-warns-against-its-lawful-but-malicious-use>)

47 NATGRID Will Prove to be Security Nightmare", The Sunday Guardian (<http://www.sunday-guardian.com/analysis/natgrid-will-prove-to-be-a-security-nightmare>)

48 Universal Declaration of Human Rights Article 12, United Nations Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights Article 17.

49 Right to Life and Liberty

the right to privacy cannot be read into the Indian constitution⁵⁰. This disregard for the right to privacy is quite at odds with some statements made by India in international fora, where it has repeatedly spoken out in defense of the right to privacy⁵¹. This only lends credence to the suspicion of civil society in relation to the lack of privacy safeguards in the mass data collection programmes of the State.

38. The right to privacy when affirmed by Courts, has been subject to restrictions. It can be curtailed only through procedure established by law, where the procedure is fair, just and reasonable⁵². It 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 Tribes⁵³. These are broad categories, in need of legislative guidance. In the absence of clear legislative safeguards and procedures meeting international standards, the right to privacy, especially in the digital medium and online platforms will remain vulnerable.
39. There is no statutory redressal mechanism in case of illegal interception and monitoring of information and communications by the State or private parties. Intelligence agencies in India are exempt from transparency enhancing laws the like RTI Act, and insist on remaining exempt from any attempts at legislative protection of privacy like the Privacy Bill of 2013.⁵⁴ A legislation providing privacy protections from the State and the private sector is needed, and such a legislation should not exempt intelligence agencies from falling within its ambit.

c UID (Unique Identification) number or 'Aadhaar'

40. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 was passed as a money bill, circumventing the majority required in the Rajya Sabha for passage. While this Act purports to make government delivery of welfare schemes more efficient, the Unique Identity Authority of India (UIDAI) is

50 (2014) 6 SCC 433

51 "Spy agencies, IB and RAW, put spanner in proposed privacy law" Hindustan Times, Nov. 2, 2013

52 Maneka Gandhi v. Union of India (1978) 2 SCR 621

53 Govind v. State of M.P 1975 AIR 1378

54 Spy agencies, IB and RAW, put spanner in proposed privacy law" Hindustan Times, Nov. 2, 2013 (<http://www.hindustantimes.com/india/spy-agencies-ib-and-raw-put-spanner-in-proposed-privacy-law/story-aAzkudi7oHHDQ2SWj3s4UO.html>)

empowered to disclose many fields of information and interception of electronic communication upon an authentication request by government agencies and private actors⁵⁵.

41. Other provisions like the National Population Register⁵⁶ and DNA Profiling Bill 2015⁵⁷ have been specifically set up with security of the State as the mandate and aim⁵⁸. Without a privacy legislation that contains redressal mechanisms, this identity number attached to demographic and biometric sensitive information is liable to be misused.

d. Encryption

42. 42. The government released a draft encryption policy in September 2015⁵⁹, The draft policy required all application service providers to deposit the private key with encrypted content to the government. This enables law enforcement and other authorised parties can access such content. Further, it required users to store the plaintext of encrypted content, to be handed over to authorised government agencies, when required. The very purpose of encryption is defeated if data is held in plain text insecurely by the user.
43. According to the License Agreement that ISPs have to enter into, the permitted upper limit for encryption strength is 40 bits in symmetric algorithms, for ISPs and individuals alike, which is an extremely weak standard.

55 Aadhaar and the right to privacy", The Hindu, Oct. 20, 2015 (<http://www.thehindu.com/opinion/columns/aadhaar-and-the-right-to-privacy/article7781020.ece>)

56 The National Population Register (NPR) is a Register of usual residents of the country; <http://censusindia.gov.in/2011-Common/IntroductionToNpr.html>

57 DNA Profiling Bill, <http://www.prsindia.org/uploads/media/draft/Draft%20Human%20DNA%20Profiling%20Bill%202015.pdf>

58 <http://cis-india.org/internet-governance/blog/indias-biometric-identification-programs-and-privacy-concerns>

59 Draft Encryption Policy, Department of Electronics and Information Technology, available at: <https://cdn.netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf>

FREEDOM OF ASSOCIATION AND ASSEMBLY ONLINE

44. Freedom of assembly and association (FOAA) is fundamental to democracy and as such is protected in the Constitution of India under Article 19. The recent trends mentioned in this submission point to the fact that the government makes consistent attempts to curtail FOAA online. For example, during the incidence of Patel community's agitation in Gujarat, the state shut down communication networks including mobile and internet.
45. For a collective to exercise its right to association and assembly, it does not have to necessarily come together in physical spaces. Increasingly, civil society groups and activists are using the internet to mobilise, disseminate information and resources and campaign online. More often, the offline threats to individuals and collectives are replicated online in the form of hate speech and intimidation from groups and individuals opposed to such views. Presently there is no law in India that protects FoAA online. However, the laws that protect us offline should extend protection online as well.
46. The most commonly cited excuse by the State for violating FoAA online and offline is the interest of national security and maintaining public order. The specific case of repeated shutdowns in Kashmir is a stark example of this. The GoI has shutdown internet and phone networks in Kashmir on multiple occasions including in July 2016, in the name of preventing the spread of misinformation and momentum through social media. Earlier, in March 2014, the internet was shut down in Jammu and Kashmir to bar HRDs and others from having access to the proceedings of UNHRC session⁶⁰. Conflict regions in the country continue to face such shutdowns whenever there are situations of public dissent and protests against the State.

a. Network Shutdowns

47. According to Special Rapporteur Frank La Rue's report on the promotion and protection of the right to freedom of opinion and expression⁶¹, Internet shutdowns violate freedom of speech. Across India such shutdowns are imposed through

60 "India shuts down internet to prevent Mirwaiz's address" Kashmir Media Service (<http://www.kmsnews.org/news/2014/03/18/india-shuts-down-internet-to-prevent-mirwaizs-address.html>)

61 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, General Assembly, A/HRC/17/27, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Section 144 of the Criminal Procedure Code⁶². Internet shutdowns mean that ISPs are instructed to snap 2G, 3G, GPRS, lease line and/or broadband services in the specified regions.

48. In September 2014, without any prior announcement, the Gujarat government had shut down mobile networks to prevent communal violence in the state⁶³. In March 2015, internet and SMS services were blocked in Nagaland for 48 hours in relation with lynching of a rape accused⁶⁴.
49. Already in 2016, there have been internet shutdowns in Jharkhand⁶⁵, Jammu & Kashmir⁶⁶. In 2015, Internet services were shut down in Nagaland⁶⁷, Gujarat, Manipur⁶⁸, Kashmir⁶⁹, Rajasthan⁷⁰. In 2013 and 2014, Internet services were

62 Section 144(1) of CrPC- 144. Power to issue order in urgent cases of nuisance of apprehended danger:

(1) In cases where, in the opinion of a District Magistrate, a Sub-divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, there is sufficient ground for proceeding under this section and immediate prevention or speedy remedy is desirable, such Magistrate may, by a written order stating the material facts of the case and served in the manner provided by section 134, direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management, if such Magistrate considers that such direction is likely to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, or an affray.

63 Internet services blocked in Vadodara after riots", The Times of India, Sep. 28, 2014 (<http://timesofindia.indiatimes.com/city/vadodara/Internet-services-blocked-in-Vadodara-after-riots/articleshow/43674499.cms>)

64 Dimapur lynching: SMS, internet services blocked in Nagaland for 48 hours" Firstpost, March 8, 2015 (<http://www.firstpost.com/politics/dimapur-lynching-sms-internet-services-blocked-in-nagaland-for-48-hours-2142227.html>)

65 Mobile Internet services cut off in Gujarat districts & Bokaro, Jharkhand" Medianama, April 18, 2016 (<http://www.medianama.com/2016/04/223-mobile-internet-ban-gujarat-bokaro/>)

66 Kashmir shut down for 3rd day, mobile internet services suspended" Hindustan Times, April 15, 2016 (<http://www.hindustantimes.com/india/handwara-firing-mobile-internet-services-suspended-in-kashmir/story-iPQHs3vdmIWx7w0uCGK8NJ.html>)

67 "Internet Blackout In Nagaland As Gruesome Video Of Lynching Surfaces; 22 Arrested" The Huffington Post, July 15, 2016 (http://www.huffingtonpost.in/2015/03/09/nagaland-lynching_n_6828442.html)

68 Why a blanket ban on the internet in troubled Manipur is not a good idea" Scroll, Sep 4, 2015 (<http://scroll.in/article/753108/why-a-blanket-ban-on-the-internet-in-troubled-manipur-is-not-a-good-idea>)

69 Jammu and Kashmir suspends Internet services in state for two days over beef controversy" Medianama, Sep. 25, 2015 (<http://www.medianama.com/2015/09/223-jammu-and-kashmir-internet-ban/>)

70 "Rajasthan blocks Internet services in some districts indefinitely" Medianama, Dec. 21, 2015 (<http://www.medianama.com/2015/12/223-rajasthan-internet-block/>)

temporarily banned in Kashmir⁷¹ , Gujarat⁷² sometimes for reasons like preventing cheating in an examination, preventing an apprehension of violence etc.

50. During the public agitation for by the Patel community for demanding reservations in education and employment in 2015, the government again, as a knee jerk reaction, blocked mobile internet services in the state to stop the spread of the movement through social media⁷³ .

.....

71 Afzal Guru hanged: Mobile internet services snapped in Kashmir" The Times of India, Feb. 9, 2015 (<http://timesofindia.indiatimes.com/india/Afzal-Guru-hanged-Mobile-internet-services-snapped-in-Kashmir/articleshow/18415453.cms>)

72 Legality of Internet shutdowns under Section 144 CrPC" Software Law Freedom Centre, <http://sflc.in/legality-of-internet-shutdowns-under-section-144-crpc/>

73 "Mobile internet services banned across Gujarat after Hardik Patel's detention" The Times of India, Sep. 9, 2015 (<http://timesofindia.indiatimes.com/india/Mobile-internet-services-banned-across-Gujarat-after-Hardik-Patels-detention/articleshow/49024649.cms>)

GENDER AND THE INTERNET

a. Access for Women

51. A significant gender gap in access to digital technologies, mediated by traditional inequalities exists in the country. Women face more familial and societal censure than men for using mobile phones or the internet⁷⁴. However, the provision of infrastructure and devices alone will not increase women's access. Multiple barriers need to be simultaneously addressed to address this divide. These include women's exclusion from technology education, lack of digital skills, social norms that favour men, financial and institutional constraints⁷⁵.
52. In some villages of Uttar Pradesh⁷⁶, Rajasthan⁷⁷ and Gujarat⁷⁸, khap panchayats⁷⁹ have banned young and unmarried women from using mobile phones. These actions further restrict women's access not just to digital technologies but also to information, speech and expression.
53. Such extra-legal actions must be seen as:
 - a discriminatory restriction on full access to digital technologies for all
 - a threat to the right to FOE
 - a violation of Article 19 of the Indian Constitution, which guarantees citizens the right to FOE. The only 'reasonable' restrictions to this right are specified in the constitution⁸⁰

74 "A Gross Misuse of the IT Act by Mumbai Police", The Wire, July 14, 2015, available at: <http://thewire.in/6390/mumbai-polices-gross-misuse-of-the-it-act/>

75 "Mobile Phones and Literacy, Empowerment in Women's Hands - A Cross Case Analysis of Nine Experiences", UNESCO, 2015, available at <http://unesdoc.unesco.org/images/0023/002343/234325E.pdf>

76 "Panchayat bans mobile phones among girls" The Time of India, Feb. 19, 2016 (<http://timesofindia.indiatimes.com/city/agra/Panchayat-bans-mobile-phones-among-girls/articleshow/51060339.cms>)

77 "Khap panchayat strikes again: Mobile phones use banned for girls in Barmer" Zee News, July 2, 2015 (http://zeenews.india.com/news/rajasthan/khap-panchayat-strikes-again-mobile-phones-use-banned-for-girls-in-barmer_1623430.html)

78 Gujarat village bans mobile phones for unmarried women" Hindustan Times, Feb. 18, 2016 (<http://www.hindustantimes.com/india/gujarat-village-bans-mobile-phones-for-unmarried-women/story-iziKwjYckgm00P8ZRBn3K.html>)

79 Khap Panchayat; <https://en.wikipedia.org/wiki/Khap>

80 Restrictions on freedom of expression (Article 19): Interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence

b. Access for Sexual Minorities

54. With Section 377 of the IPC (deals with unnatural offences—whenever voluntarily has carnal intercourse against the order of nature with any man, woman or animal, shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to 10 years, and shall also be liable to fine) currently in place, sexual minorities are vulnerable to blackmail and threats of being outed. In this scenario, the internet plays a big role as a safe space as well as a source of information. But this access will not be safe or secure unless their right to anonymity and right to privacy is guaranteed.

c. Consent

55. In the last two years, there have been several cases of ‘rape videos’ being circulated in digital spaces, particularly on messaging services, social media and adult sites.⁸¹ These are cases of actual rapes which are recorded and circulated by the perpetrators and are used to blackmail or threaten women into silence⁸². Several of these cases are now before the Supreme Court, which has directed the GoI to take action.

56. Three provisions of law are used to punish rape and the production and distribution of rape videos. Section 376 of the IPC deals with the rape itself, while either Section 67 (obscenity) or Section 66E (non-consensual images) of the IT Act are in place to punish its filming and digital circulation.

57. Rape videos are typically legally classified as ‘obscene’ images by placing them under 67 of the IT Act. National Crime Records Bureau (NCRB) data from 2008 to 2014 clearly establishes that Section 67 of the IT Act is the 2nd highest used section of the IT Act⁸³.

81 Muzaffarnagar on boil again as rape video goes public, BJP leader jumps in” Indian Express, Jan. 19, 2016 (<http://indianexpress.com/article/india/india-news-india/muzaffarnagar-on-boil-again-as-rape-video-goes-public-bjp-leader-jumps-in/>)

82 MBA student from Jindal Global University alleges sexual assault in campus, moves SC demanding CBI probe” LiveLaw, May 20, 2015 (<http://www.livelaw.in/mba-student-from-jindal-global-university-alleges-sexual-assault-in-campus-moves-sc-demanding-cbi-probe/>)

83	Number of cases Section 67	Number of cases Section 66E
	2008	105
	2009	139
	2010	328

-
- 58. The production and distribution of rape videos are, like rape itself, crimes that violate an individual's dignity and ability to consent. They must be legally recognised as such, rather than primarily as 'obscene' images. There is a section in the IT Act– 66E – to address non-consensual sexual images, but this is grossly underused.
 - 59. Section 66E, which punishes the capturing, publishing or transmitting of images of private areas without consent, must be used to address the production and distribution of rape videos and other non-consensual sexual images.⁸⁴ Consent is an intrinsic aspect of privacy, which the section explicitly recognises. Strengthening the use of section 66E will also strengthen the right to privacy and recourse to legal remedies to protect this right.
 - 60. Women in India use digital spaces for many forms of expression, including sexual expression. Young women, in particular, negotiate freedom and censure by using online spaces to challenge cultural taboos and social restrictions around sexuality, relationships and self-determination.⁸⁵ Legal distinctions between the 'consensual' and the 'non-consensual' must be strengthened to enable freedom of expression, including sexual expression.
 - 61. Incidents of regressive and ignorant usage of terminology without clarifications or

2011	496
2012	589
2013	1203

84 This section specifies that "whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished."

85 EROTICS: An exploratory research project into sexuality and the internet, Association for Progressive Communications, available at: <https://www.apc.org/en/system/files/EROTICS.pdf>

CYBER CRIME AND SEXUAL EXPLOITATION

thorough research have been recorded in relation to cybercrime. NCRB, in its report Crime in India 2014, had published a category of criminals as 'sexual freaks'. No definition or clarifications were provided in the preceding sections. This type of loose and disrespectful categorisation may lead to discrepancies in recording of cases and trial⁸⁶.

62. The government has been obstinate in denying Special Rapporteurs' country visit

.....
⁸⁶ Crime in India Report 2014, National Crime Records Bureau, Ministry of Home Affairs, available at: (<http://ncrb.nic.in/StatPublications/CII/CII2014/Compendium%202014.pdf>)

INTERNATIONAL MECHANISMS

requests. The Special Rapporteur on the right to Freedom of Opinion and Expression has never received an invitation for country visit. The Special Rapporteur on the right to Freedom on Peaceful Assembly and Association had made a last request in September 2014, which was denied and is still pending⁸⁷.

63. Ensure effective implementation and monitoring of programmes aimed at increasing

.....
⁸⁷ United Nations Office of the High Commissioner for Human Rights, Country and other visits by Special Procedures Mandate Holders since 1998, <http://www.ohchr.org/EN/HRBodies/SP/Pages/CountryvisitsF-M.aspx>

RECOMMENDATIONS TO THE GOI

effective implementation & monitoring of programmes aimed at increasing universal, affordable, unhindered and democratic access to information and to the internet, in accordance with international human rights standards.

64. Further implementation of the existing domestic programmes that aim at achieving accessibility, availability and transparency of information in the public domain.
65. Ensure, in its initiatives to make government websites accessible for the people with disabilities, that the content follows W3C guidelines and is updated regularly.
66. Ensure that restrictions placed on the exercise of human rights including the right to freedoms of expression, assembly and association on the internet need constitutional and international guarantees.
67. Ensure removal of restrictions for expression of political and religious dissent without the fear of persecution.
68. Commit to eliminate impunity enjoyed by the non-state actors, engaged in persecuting minorities and dissenters.
69. Ensure that a comprehensive legislation is put in place to provide strong protections of the right to privacy.
70. Recognise the importance of anonymity in promoting and protecting the rights to freedom of expression and privacy and refrain from passing laws and policies that curb anonymity.
71. Ensure that blocking and filtering of content on the Internet is not carried out without a valid court order and in accordance with international standards.
72. Prescribe clear limits on state surveillance in accordance with international standards, and discontinue bulk collection of citizen data, which violates the right to privacy.
73. Comply with orders passed by the Courts to remove the mandatory requirement of the

Aadhaar for delivery of welfare services by the government. Additionally, prohibit UIDAI from disclosing biometric information or detailed fields of demographic information to government bodies or private bodies seeking authentication. Place strong penalties and create redressal mechanisms for breach of data either by sub-contractors, private parties or government agencies.

74. Refrain from interfering with the use of encryption and desist from directing manufacturers of software and hardware to insert backdoors.
75. Address violation of FOAA in compliance with international mechanisms and standards.
76. Immediately end the use of section 144 of the IPC to justify network shutdowns in the name of law and order, as such shutdowns negatively affect access to information, transfer and crucial communication services in the area, in addition to emergency humanitarian services.
77. Take strong measures against community bodies that impose restrictions on the use of technology, especially mobile phones, especially on women.
78. Take steps to respect, promote and protect full access for all women, particularly in contexts where non-legal restrictions are imposed on access to the internet.
79. Take appropriate legislative and procedural measures to promote and protect full access to the internet for women and sexual minorities to the internet.
80. Ensure that rights and laws are such that they keep open for women and sexual minorities the possibilities of exploring digital spaces to express themselves, including their sexuality.
81. Strengthen the use of Section 66E of the IT Act, in dealing with cases of harassment involving non-consensual circulation of text, videos, etc, leading to privacy violations.
82. Ensure that terminologies used in national cyber-crime reports and records are explained clearly and avoid usage of regressive and potentially harmful terms.
83. Extend invitations to all thematic UN Special Rapporteurs, particularly related to the

rights of freedom of opinion, expression, assemblies, association, privacy and HRDs.

84. Ensure that National Human Rights Institutions incorporate internet rights as part of their approach to human rights, as articulated by the UN Human Rights Council.
85. Adopt and comply with the principles of international human rights and UN mechanisms such as the UN Special Procedures and treaty bodies, not only to protect and promote human rights in the country but also to continue to play leadership position in persuading other developing countries.

