IFF's written contribution to the

United Nations' Human Rights Committee ahead of India's 4th Periodic Review

Internet Freedom Foundation

INTERNET FREEDOM FOUNDATION

Internet Freedom Foundation I-1718, Third Floor,
Chittaranjan Park, New Delhi 110019

Recommended Citation: Disha Verma, Tejasi Panjiar & Gayatri Malhotra, “IFFs written contribution to the United Nations' Human Rights Committee ahead of India’s 4th Periodic Review", Internet Freedom Foundation, June 03, 2024.

Internet Freedom Foundation (“IFF”) is a registered charitable trust which advocates for the digital rights of Indians. Our mission is to ensure the growth of digitisation with democratic rights guaranteed under the Constitution of India.

Authors:

Disha Verma is an Associate Policy Counsel at IFF. A lawyer by training, Disha spent nearly three years working in health policy focusing on community health and disease response at the national and global level, before transitioning to tech policy. At IFF, she engages with state deployment of technologies in welfare delivery, surveillance and public administration through a critical and rights-affirming lens.

Tejasi Panjiar is the Associate Policy Counsel at the IFF. She did her Post-graduation in Public Policy at O. P. Jindal Global University. She pursued her undergraduate course in Political Science (Hons.) from Kamala Nehru College, University of Delhi. Her work at IFF covers issues of privacy and data protection, platform governance, cyber security, and telecom policy.

Gayatri Malhotra is the Associate Litigation Counsel at the Internet Freedom Foundation. She is an alumna of the Jindal Global Law School. Her work at IFF covers internet shutdowns, online censorship, the right to information, privacy, and data protection.

We would like to thank Executive Director, Prateek Waghre, Community and Fundraising Associate, Purvai Dwivedi and Freedom Innovation Fellow, Shravani N Lanka for their assistance.

Table of Contents

United Nations Human Rights Committee
141st session June 03, 2024

Internet Freedom Foundation's written contribution ahead of India's 4th Periodic Review

Internet Freedom Foundation ("**IFF**") is a registered charitable trust that works to advance constitutional guarantees in India, especially as they relate to digital rights and freedoms, through strategic litigation, government engagement, and civic advocacy. We work across a wide spectrum of issues, with expertise in free speech, platform governance, electronic surveillance, data protection, net neutrality and innovation. We make this submission ahead of the United Nations Human Rights Committee's ("**UNHRC**") review of State parties to highlight key areas of concerns regarding India's compliance with the International Covenant on Civil and Political Rights including new measures and developments relating to the implementation of the Covenant for the period 2019–2024, with the objective of aiding and informing the Committee's review process and outcome report(s). We consent to the publication of this submission on the Committee's website.

Summary of findings

Increasing adoption of the internet in a society can signal a continuing belief that it has the potential to make our lives better. But on a closer look, we see that it can also as easily be wielded as a tool of arbitrary executive control by governments, which can stifle rights and freedoms, amplify socio-economic differences, and further deepen the digital divide. In the last five years, abundant instances of indefinite and disproportionate internet shutdowns, increasing censorship, increasingly pervasive e-surveillance, threats to net neutrality, tech-enabled gender violence and hate speech, and a number of other examples indicate that while Indians are online, our engagement with the internet is not necessarily meaningful, fructuous, or even wilful. India's move towards large-scale digitalisation necessitates a critical look at law and policy instruments governing the space—which commonly appear to be vague, arbitrary, exclusionary, or fail to place human rights at their core. New laws and digital interventions seem to share the lack of public consultations and stakeholder participation. A spike in public-private partnerships across sectors is weakening transparency and accountability mechanisms. The 2019-2024 window is a crucial time for a deep assessment of the state of privacy, dignity, free speech, and several other constitutional guarantees of Indian citizens, their interpretation in Indian courts, and the need for rights-based legislation in the digital sphere. We thank the Committee for undertaking the periodic review of India and giving civil society organisations like IFF the opportunity to draw from their work and provide diverse perspectives to the process.

Issue-wise analysis

I. An introduction to "Digital India"

Access to the internet is globally seen as a significant human right with invaluable benefits in day-to-day life.[1] Especially in context of developing countries, internet connectivity can boost businesses, education, information symmetries, and thus, overall socio-economic development. At present, over half the Indian population has access to the internet.[2] But for a country like India, wider internet adoption does not necessarily imply meaningful access to the internet. India suffers from a gaping digital divide, where factors of low literacy and unfamiliarity with emerging technological tools can impede many population groups from reaping the benefits of the internet and digital technologies recreationally as well as for better quality of life.[3] A major event in the last five years that revealed the depth and extent of the Indian digital divide is the COVID-19 pandemic, where increased digitalisation and reliance on online tools across sectors like education, labour, and health, forced many to fall through the cracks.[4]

Data from the Telecom Regulatory Authority of India reveals that, as of 2023, 95.66% of total broadband subscribers (wired and wireless) and ~60% of the Indian population access the internet through their wireless devices (mobiles and dongles).[5] According to The Mobile Gender Gap Report 2022 published by the Global System for Mobile Communications Association, smartphone ownership and mobile internet use in India have grown steadily for men since 2019, however, it still remains uncommon among women.[6] Data from the National Family Health Survey–5 (2019-21) found that only one in three women in India (33%) have ever used the internet, compared to more than half (57%) of men.[7] The gendered barriers are even more stark in rural parts of the country, with men twice as likely as women to have used the internet

---

[1] Hjort, Jonas, and Lin Tian. "PEDL Synthesis Paper 6: Firms and Skills: The Evolution of Worker Sorting." Policy Experimentation and Evaluation in Developing Countries (PEDL) Synthesis Paper, no. 6. London: Centre for Economic Policy Research, August 19, 2021. https://pedl.cepr.org/sites/default/files/Synthesis%20Paper%20SP6%20Jonas%20Hjort.pdf.

[2] "Rural India Accounts for 53% of Internet Consumption: Report." Fortune India, February 27, 2024. Accessed May 30, 2024. https://www.fortuneindia.com/macro/rural-india-accounts-for-53-of-internet-consumption-report/115938.
See also: "Over 50% Indians are active internet users now; base to reach 900 million by 2025: report." The Hindu, May 4, 2023. Accessed May 29, 2024. https://www.thehindu.com/news/national/over-50-indians-are-active-internet-users-now-base-to-reach-900-million-by-2025-report/article66809522.ece.

[3] Rohin Garg. "Improving Internet Access: An Explainer." Internet Freedom Foundation, April 7, 2021. Accessed May 29, 2024. https://static.internetfreedom.in/improving-internet-access-an-explainer/.

[4] Rajul Sharma. "The digital platform-driven COVID-19 vaccine drive amidst a digital divide: Lessons from India." Leiden Law Blog, January 13, 2021. Accessed May 30, 2024. https://www.leidenlawblog.nl/articles/a-digital-platform-driven-COVID-19-vaccine-drive-amidst-a-digital-divide-lessons-from-india. See also: Murali Krishnan. "Millions of Indian Children Affected by COVID-Related School Closures, Digital Divide." The Wire, December 29, 2021. Accessed May 30, 2024. https://thewire.in/education/millions-of-indian-children-affected-by-COVID-related-school-closures-digital-divide. See also: Nikore, Mitali. "How COVID-19 Deepened Gender Fault Lines in India." Economic and Political Weekly, December 17, 2022. Accessed May 30, 2024. https://www.epw.in/engage/article/how-covid-19-deepened-gender-fault-lines-indias.

[5] "The Indian Telecom Services Performance Indicators October-December 2023." Telecom Regulatory Authority of India, https://www.trai.gov.in/sites/default/files/QPIR_23042024_0.pdf. See also: "Total Population by Country 2024." World Population Review, https://worldpopulationreview.com/countries.

[6] "The Mobile Gender Gap Report 2022." GSMA, June 2022. Accessed June 1, 2024. https://www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf.

[7] "The digital divide and is it holding back women in India?" Hindustan Times, January 16, 2022. Accessed May 30, 2024. https://www.hindustantimes.com/ht-insight/gender-equality/the-digital-divide-and-is-it-holding-back-women-in-india-101641971745195.html.

(49% vs 25%).[8] For more analysis on India's internet connectivity data, please refer to IFF's periodic reports titled "Connectivity Tracker".[9] To combat the digital divide, the union government had launched two ambitious schemes—PMGDISHA and BharatNet, but both schemes significantly lag behind in fulfilling their targets.[10] Repeated reliance of the government on digitalisation and technology-first solutions has also not helped bridge the gaps.

The incumbent government's flagship 'Digital India' programme launched by the Union Ministry of Electronics & IT ("**MeitY**") to "*transform India into a digitally empowered society and knowledge economy*" struggled with addressing the foundational encumbrances like infrastructural capacity, tech-preparedness, and the aforesaid digital divide. The programme envisions *inter alia* large-scale digitalisation across sectors and erecting 'digital public infrastructure' for collaborative public-private provisioning of digital services. Naturally, an exercise of this magnitude also envisions large-scale data collection and processing. Without adequate data literacy and empowerment, populations may be confronted with exploitative data sharing and collection practises in the absence of informed consent or due compensation.

The foundational fallacy of India's ambitious digitalisation programme which relies so heavily on citizen data collection, is the lack of an active data protection law. The Digital Personal Data Protection Act ("**DPDPA**"), 2023 was passed and notified in 2023 after a long and winding journey through committees and consultations. Yet, its final version seemed unrecognisable and was never opened up for public scrutiny and consultation. The DPDPA, 2023 has not yet been implemented, and the Rules set to operationalise many of its provisions have not seen the light of day. In its present form, the Act falls short on many counts, so even when it is implemented, India's overarching data protection law will suffer from holes and pitfalls.[11]

---

[8] "Stage Has Been Set for Gender Equity in Digital India." UNFPA India, March 22, 2023. Accessed May 30, 2024. https://india.unfpa.org/en/news/stage-has-been-set-gender-equity-digital-india.

[9] "Connectivity Tracker." Internet Freedom Foundation. Accessed May 31, 2024. https://internetfreedom.in/tag/connectivitytracker/.

[10] Under PMGDISHA, a program aimed to digitally educate 6 crore individuals by March 31, 2019, only 4.70 crore candidates have received certification as of December 31, 2023. As of November 29, 2023, 2,12,081 Gram Panchayats have been made service-ready according to the Minister of State for Communications. However, data.gov.in reveals that just 1,93,472 service ready are service ready as of November 30, 2023 with no apparent explanation for the delta. See: Tejasi Panjiar and Disha Verma. "Legislative Brief on Digital Rights for Budget Session 2024." Internet Freedom Foundation, January 24, 2024. Accessed May 29, 2024. https://internetfreedom.in/legislative-brief-2024-budget/; See also: Bhandari, Vrinda. "Improving Internet Connectivity During COVID-19." Digital Pathways at Oxford Paper Series; no. 4. Oxford, United Kingdom, 2020. Accessed May 31, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3688762.

[11] Anushka Jain and Prateek Waghre. "IFF's First Read of the Draft Digital Personal Data Protection Bill 2023." Internet Freedom Foundation, August 3, 2023. Accessed May 29, 2024. https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/.

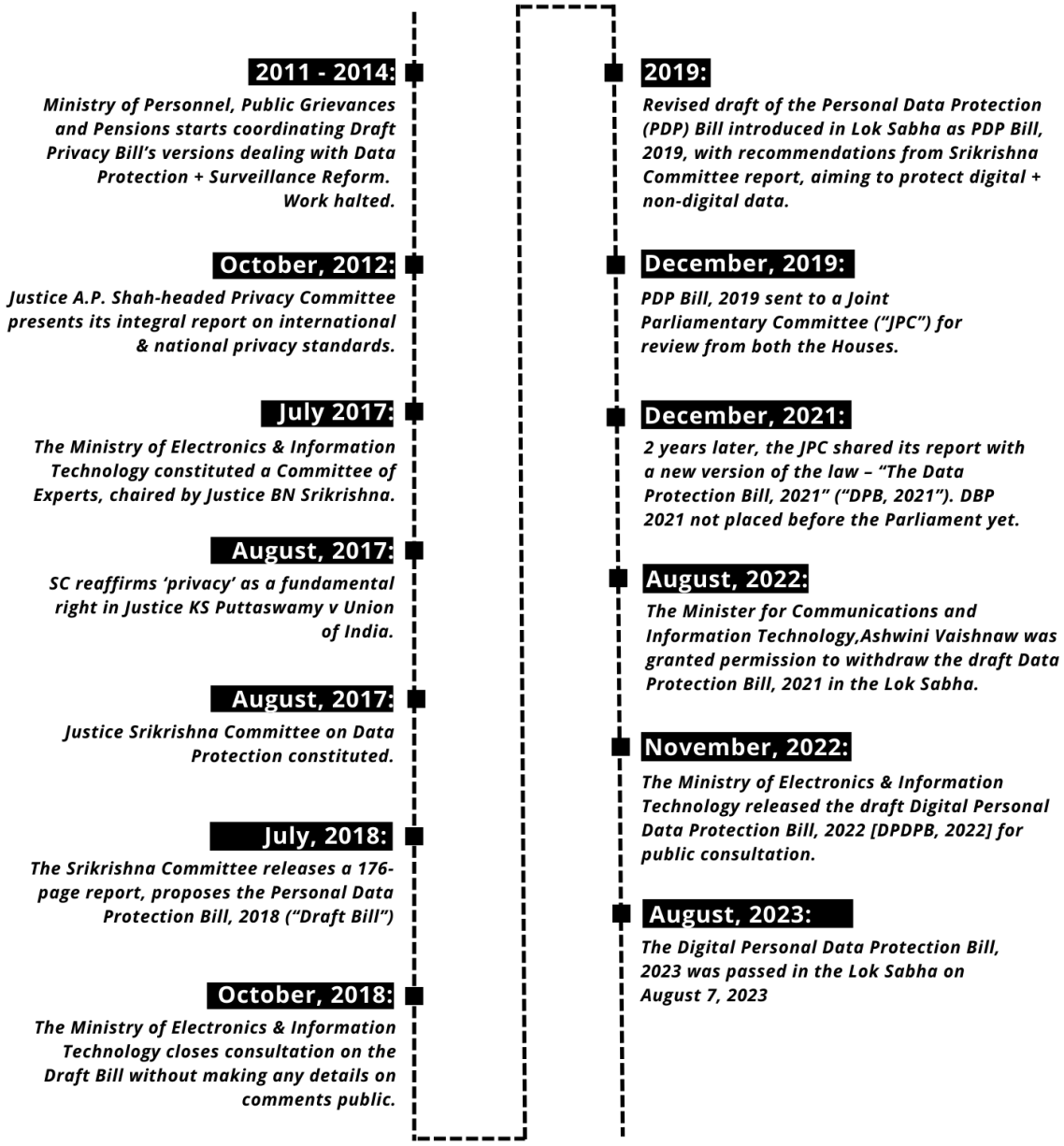

Image: Timeline of data protection legislation since 2011

Another fallacy of the 'Digital India' programme is in its attempt to digitalise the Indian welfare sector despite informed and grounded pushback. Social security guarantees like health access, employment, or education are being made contingent on how well populations seeking welfare are able to use and understand technology.[12] This, in itself, is a deeply flawed approach bound to deepen existing differences. Take for instance India's National Rural Employment Guarantee Act, 2005 ("**NREGA**"), a watershed social security legislation founded in public advocacy and civil society efforts that has acted as an employment safety net for economically underprivileged families for nearly two decades.[13] In recent

[12] Supra at 4.
[13] Kaajal Joshi. "15 Years In: The MGNREGA Story." Participatory Research in Asia, March 2021. Accessed May 30, 2024.

times, this framework has been undermined at a rapid pace due to the introduction of programmatic digital interventions and technological "solutions" which are strongly opposed by scheme beneficiaries.[14] Digitalising how beneficiaries engage with NREGA has potentially entrenched the scheme with an additional set of issues around access, inaccuracy, exclusion, and disenfranchisement.

A similar governance approach is seen in the domains of agriculture and health too, through the introduction of 'AgriStack' and 'HealthStack'. The AgriStack is a collection of technologies and digital databases to help India's farmers and the agricultural sector navigate issues of poor access to credit and wastage in the agricultural supply chain.[15] Farmers, the primary stakeholders, have been left out of the policymaking process by design.[16] Under HealthStack, an array of new programmes such as the Universal Health ID, Health Data Management Policy, and United Health Interface have been launched in a short window of time and without adequate stakeholder consultation.[17,18,19] We have repeatedly pointed out issues of privacy, exclusion, and administrative coercion prevalent in the HealthStack framework, and yet unique IDs continue to be created for seemingly anyone seeking health security or services in India, sometimes without consent.[20,21]

Another strong structural push from the union government without due consideration of its human rights implications has been 'digital public infrastructure' ("**DPI**"). While India has rolled out and invested in DPI projects on a significant scale in the last couple of years alone, there is not much critical analysis or feedback on how distinctly vague, ambiguous, unaccountable, and non-transparent our DPI approach has been. The union government has preferred a wide (if any) definition for what constitutes DPI, where state-backed projects can be hailed as DPI without subtext or seemingly much of a criteria. Indian DPIs, at their core, are built on public-private partnerships ("**PPP**"s) and are deployed in the public sector to reach a maximum possible population cover. There is no anchoring law, policy, or act of Parliament governing such vast public systems or providing baseline safeguards. There is little publicly available critical and human rights analysis on the infrastructure. The success or efficacy of the PPP model in provisioning state functions is yet to be convincingly demonstrated.[22] Yet, the push continues.

---

https://www.pria.org/knowledge_resource/1621863093_1618822426_1618816284_15%20years%20in-the%20mgnrega%20story1.pdf.

[14] Disha Verma. "No place for tech: How digital interventions in NREGA are undermining rural social security." Internet Freedom Foundation, February 20, 2024. Accessed May 29, 2024. https://internetfreedom.in/no-place-for-tech-in-nrega/.

[15] Rohin Garg. "The AgriStack: A Primer." Internet Freedom Foundation, December 4, 2020. Accessed May 28, 2024. https://internetfreedom.in/the-agristack-a-primer/.

[16] Rohin Garg. "A Thoroughly Bad IDEA: Our comments on the AgriStack Consultation Paper." Internet Freedom Foundation, July 6, 2021. Accessed May 28, 2024. https://internetfreedom.in/iff-response-to-the-idea-paper-on-agristack/.

[17] "Ayushman Bharat Digital Mission." Accessed May 28, 2024. https://ndhm.gov.in/health_management_policy.

[18] "Explainer on the Unique Health Identifier Rules, 2021." Internet Freedom Foundation, January 19, 2021. Accessed May 29, 2024. https://drive.google.com/file/d/1gza8WXnY9nLfB2BdRWyRe32Y--KxyJ-P/view.

[19] Anushka Jain. "Civil Society's second opinion on a UHI prescription." Internet Freedom Foundation, January 14, 2023. Accessed May 28, 2024. https://internetfreedom.in/civil-societys-second-opinion-on-a-uhi-prescription/.

[20] Rohin Garg. "An Explainer on the Unique Health Identifier Rules, 2021." Internet Freedom Foundation, January 19, 2021. Accessed May 28, 2024.https://static.internetfreedom.in/health-id-rules-explainer/. See also: Rohin Garg. "Analysing the NDHM's Health Data Management Policy: Part 2." Internet Freedom Foundation, July 15, 2021. Accessed May 29, 2024. https://static.internetfreedom.in/analysing-the-ndhms-health-data-management-policy-part-2/.

[21] Sarthak Dogra. "Took COVID vaccine using Aadhaar? Your National Health ID has been created without your permission." India Today, May 24, 2021. Accessed May 29, 2024. https://www.indiatoday.in/technology/features/story/took-COVID-vaccine-using-aadhaar-your-national-health-id-has-been-created-without-your-permission-1806470-2021-05-24.

[22] Subhomoy Bhattacharjee. "Why PPP Projects fail." Business Standard, April 20, 2018. Accessed May 29, 2024.

It is against this context that we make our submissions to the Committee. In the following sections, we enumerate, highlight, and analyse India's extent of compliance with Articles and principles enshrined in the ICCPR and the key rights issues associated with them, from the lens of digital rights and freedoms.

II. Gendered Harms on the Internet

Persistent incidents of sexual harassment and doxxing have made social media platforms highly unsafe and toxic for women, which may lead some of them to disengage from social media altogether. In a distressing incident in early 2020, teenage male students from New Delhi were called out for sharing sexualized images of young women, including girls below the age of 18, on an Instagram group called 'Boiz Locker Room.'[23] Media reports suggested that the participants used the group to sexualise images posted by girls on their social media accounts, and even shared morphed images.[24] Reports indicate that in addition to non-consensually sharing images, they made misogynistic remarks objectifying the girls and even threatened to leak nude images of the girls who exposed the group.[25]

On July 4, 2021, multiple X (formerly Twitter) accounts posted screengrabs from an application hosted on GitHub titled "Sulli Deals".[26] The app shared photographs and social media handles of more than 80 Indian Muslim women without their consent, and showcased their information in a way that the user could "claim a 'sulli", which is a derogatory term used by the right wing community in India for Muslim women, as the "*deal of the day*." On January 1, 2022, an application titled "Bulli Bai" surfaced on the internet, showing pictures of Muslim women being auctioned as "*Your Bulli Bai of the day*."[27] As was found out later, this app was hosted by a 21 year old students, also on GitHub.[28] While there was no actual auction of any women involved, the objective of this app was to target, dehumanise, and intimidate women belonging to a minority religion. IFF wrote to the National Commission of Women, Delhi

https://www.business-standard.com/article/beyond-business/why-ppp-projects-fail-118042000018_1.html.
See also: Gulzar Natarajan. "Revisiting the debate on PPPs." Urbanomics, June 28, 2017. Accessed May 28, 2024. http://gulzar05.blogspot.com/2017/06/revisiting-debate-on-ppps.html. See also: Nina Shapiro. "The Hidden Cost of Privatization." Institute for New Economic Thinking, June 13, 2017. Accessed May 28, 2024. https://www.ineteconomics.org/perspectives/blog/the-business-of-government.

[23] Devdutta Mukhopadhyay. "The Internet Should Not Become a Boys Club." Internet Freedom Foundation, May 7, 2020. Accessed May 30, 2024. https://internetfreedom.in/the-internet-shouldnt-be-a-boys-club/.

[24] Mahender Singh Manral. "Bois Locker Room case: 5 boys questioned over messages on Instagram group." The Indian Express, May 6, 2020. Accessed May 29, 2024. https://indianexpress.com/article/cities/delhi/bois-locker-room-case-5-boys-questioned-over-messages-on-instagram-group-6396040/.

[25] Nishtha Gupta. "Bois Locker Room: Delhi schoolboys create group to share lewd photos, chats on classmates." India Today, May 5, 2020. Accessed May 29, 2024. https://www.indiatoday.in/india/story/bois-locker-room-delhi-schoolboys-create-group-to-share-lewd-photos-chats-on-classmates-1674303-2020-05-04.

[26] Anushka Jain and Yashaswini. "Women's safety on the Internet has to account for intersectionality." Internet Freedom Foundation, July 19, 2021. Accessed May 29, 2024. https://internetfreedom.in/womens-safety-on-the-internet-intersectionality/.

[27] Anandita Mishra. "Amina writes to the National Commission for Women and the Telangana State Women's Commission against targeted harassment of Muslim women." Internet Freedom Foundation, January 11, 2022. Accessed May 30, 2024. https://internetfreedom.in/iff-assists-amina-targeted-by-bulli-bai-app/.

[28] Arvind Ojha. "Bulli Bai App Creator Detained: Delhi Police." India Today, January 8, 2022. Accessed May 29, 2024. https://www.indiatoday.in/india/story/bulli-bai-app-creator-detained-delhi-police-1896681-2022-01-06.

Commission for Women, Delhi Police and the Mumbai Police noting the privacy and safety risks of such interfaces and requesting an expeditious investigation into the apps.[29]

According to Reporters Without Borders, there has been a 35% rise globally in women journalists being sent to prison for their work.[30] There have also been attempts to intimidate women journalists covering conflicts that were sensitive in nature.[31] As per a recent test of platform reporting mechanisms carried out by Global Witness and IFF, real-life pieces of content that targeted women on the basis of gender, some of which included Islamophobic, racist, and casteist hate, were kept live on YouTube and Indian microblogging site Koo in both the US and India despite violating companies' own policies.[32] The findings that prominent platforms are enabling misogynistic hate online come against the backdrop of a surge of online violence against women and girls in recent years, threatening women's safety, leading to serious and long-lasting mental health impacts, silencing women in online spaces and creating a chilling effect on their engagement in public and political life, from journalism to leadership roles.[33]

III. Censorship of Communal Speech Online

In August 2023, a video showing alleged misconduct by a school teacher in Muzaffarnagar, UP, came to light.[34] This video reportedly shows her instructing students to abuse and physically harm a fellow student, purportedly due to the student's Muslim identity. The incident sparked outrage, leading to demands for an investigation and legal action against the teacher. Reports also emerged of X taking down tweets about the incident, including those from journalists, in response to takedown requests from the Indian Government.[35] The Ministry of Information and Broadcasting (**"MIB"**) has in some instances resorted to the emergency blocking power under Rule 16 of the IT Rules 2021.[36] Notably, emergency

[29] "Representation to National Commission for women requesting further action on the recent incident wherein the photographs and social media handles of Muslim women were auctioned." Internet Freedom Foundation, July 17, 2021. Accessed May 30, 2024. https://drive.google.com/file/d/1GlRY0sA497pXbSZpvw5WpIf8MxUOTgGt/view. See also: "Representation to Delhi Commission for Women requesting further action on the recent incident wherein the photographs and social media handles of Muslim women were auctioned." Internet Freedom Foundation, July 17, 2021. Accessed May 30, 2024. https://drive.google.com/file/d/1XXquVPbXf-12Wv9Z797N5jQFgpzWCAJ8/view. See also: "Request to Deputy Commissioner of Police for expeditious investigation in the 'Sulli Deals' incident." Internet Freedom Foundation, October 29, 2021. Accessed May 30, 2024. https://drive.google.com/file/d/1clfu8cJ2T8DQV0wOjSCYG1XjB_QfmXDa/view. See also: "Request to Deputy Commissioner of Police for expeditious investigation in the "Bulli Bai" & "Sulli Deals" incident." Internet Freedom Foundation, January 3, 2022. Accessed May 30, 2024. https://drive.google.com/file/d/1HhUqZWe-L3x_Z_LCt_fGvrsgoU3h3ACk/view.

[30] "RSF's 2022 World Press Freedom Index: New Era of Polarisation." Reporters Without Borders (RSF). Accessed May 31, 2024. https://rsf.org/en/rsf-s-2022-world-press-freedom-index-new-era-polarisation.

[31] Nupur Basu. "Women Journalists Trolled and Targeted in India." Commonwealth Equality Network, May 12, 2022. Accessed May 31, 2024. https://commonwealth.sas.ac.uk/blog/women-journalists-trolled-and-targeted-india.

[32] Tejasi Panjiar and Prateek Waghre. "[Report] Letting Hate Flourish: YouTube and Koo's lax response to the reporting of hate speech against women in India and the US." Internet Freedom Foundation, February 1, 2024. Accessed May 29, 2024. https://internetfreedom.in/report-misogynistic-hate-speech/.

[33] "How Technology Facilitated Gender-Based Violence & Impacts Women and Girls." United Nations Regional Information Centre for Western Europe (UNRIC), November 29, 2023. Accessed June 1, 2024. https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/.

[34] Krishnadas Rajagopal. "SC directly criticises Uttar Pradesh in case of teacher goading students to slap Muslim classmate." The Hindu, January 12, 2024. Accessed May 31, 2024. https://www.thehindu.com/news/national/muzaffarnagar-slapping-case-sc-directly-criticises-uttar-pradesh-in-case-of-teacher-goading-students-to-slap-muslim-classmate/article67733661.ece.

[35] Sohina Pawah. "The Curious case of censorship in the aftermath of Muzaffarnagar viral video." The Leaflet, September 9, 2023. Accessed May 31, 2024. https://theleaflet.in/the-curious-case-of-censorship-in-the-aftermath-of-muzaffarnagar-viral-video/.

[36] Internet Freedom Foundation (@internetfreedom). 2023. https://twitter.com/internetfreedom/status/1696083969559658640.

powers can only be exercised in cases "for which no delay is acceptable." Secondly, it cannot be said to fall within the ambit of Section 69A, which is arguably narrower than Article 19(2). The MIB denied access to blocking orders, citing the national security exemption under Section 8(1)(a) of the Right to Information ("**RTI**") Act, 2005 and Rule 16 of the The Information Technology (Procedure And Safeguards For Blocking For Access Of Information By Public) Rules, 2009 ("**2009 Blocking Rules**") which constitute a separate and distinct takedown regime.[37] RTIs filed by IFF revealed that MeitY and MIB issued orders of censorship but the reason for the same was withheld.[38]

In May 2024, a post by Bharatiya Janata Party's (**"BJP"**) Karnataka unit on X triggered nationwide outrage due to its communal attack on the Indian National Congress. The Karnataka Police, after being directed to do so by the ECI, asked X to take down the controversial post by the BJP Karnataka account.[39] It is worth mentioning that the directions issued by the ECI came after the post had garnered 9.2 million views and 13,000 reshares.[40] On May 14, the Election Commission of India (**"ECI"**) released an action taken report on the enforcement of the Model Code of Conduct ("MCC"). Critical gaps identified in ECI's actions include its delayed (and often absent) decision on divisive statements made by the candidates "on communal, caste, regional language divide, or on the sanctity of the Constitution of India."[41]

IV. State of Privacy, Data Protection, and Surveillance

1. The Puttaswamy standard

In *Justice (Retd.) K. S. Puttaswamy v. Union of India [(2017) 10 SCC 1]* ("**Puttaswamy-I**"), a nine-judge bench of the Indian Supreme Court unanimously affirmed that the right to privacy is a fundamental right guaranteed under Part III of the Constitution of India, holding that privacy is an integral part of Articles 14, 15, 19, and 21.[42] It emphasised that the State must formulate a robust data protection regime by "carefully balancing" individual privacy with legitimate state concerns. *Puttaswamy-I* also noted India's obligations under international law, recognizing "privacy as a fundamental constitutional value" as part of India's commitment to a global human rights regime. It noted obligations under the 1966 International Covenant on Civil and Political Rights ("**ICCPR**") to "*respect, protect, and fulfill its norms*."[43] The duty

[37] Tanmay Singh. "Revealed: MeitY and MIB admit to ordering censorship of internet posts talking about the Muzaffarnagar slapping incident; but refuse to say why because of 'national security'." Internet Freedom Foundation, October 5, 2023. Accessed May 30, 2024. https://internetfreedom.in/muzaffarnagar-slapping-incident-censorship/

[38] Tanmay Singh. "Revealed: MeitY and MIB admit to ordering censorship of internet posts talking about the Muzaffarnagar slapping incident; but refuse to say why because of 'national security'." Internet Freedom Foundation, October 5, 2023. Accessed May 30, 2024. https://internetfreedom.in/muzaffarnagar-slapping-incident-censorship/.

[39] "EC asks X to take down BJP Karnataka's video post targeting Muslims." The Indian Express, May 07, 2024. Accessed May 31, 2024. https://indianexpress.com/elections/ec-bjp-karnataka-x-post-muslims-9314058/.

[40] "Remove BJP tweet targeting Muslims, Karnataka police issue notice to X." The Indian Express, May 07, 2024. Accessed May 31, 2024. https://indianexpress.com/article/cities/bangalore/remove-bjp-tweet-targeting-muslims-karnataka-police-notice-x-9314195/.

[41] "EC Pulls Up BJP Karnataka for Post on Muslims." The Indian Express, May 7, 2024. Accessed May 31, 2024. https://indianexpress.com/elections/ec-bjp-karnataka-x-post-muslims-9314058/.

[42] Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[43] India did not file any reservation or declaration to Article 17, though reservations were made against Articles 1, 9, and 13.

of a State to respect mandates that it must not violate the right, while the duty to protect mandates that the Government must protect it against interference by private parties[44].

Over the years, the Supreme Court consistently acknowledged that the principles enshrined in the UDHR and ICCPR are integral to India's constitutional framework. The Court has consistently endorsed and applied the proportionality test, akin to the three-part test of the ICCPR to evaluate restrictions on freedom of expression. The five-prongs of the proportionality test are: (a) existence of a legitimate state interest; (b) suitability (the existence of a rational nexus between the measure and goal); (c) necessity (the rights-infringing measure must be the least restrictive way of achieving the goal); (d) proportionality *stricto sensu* (there must be a balance between the extent of infringement and strength of the goal); (e) the existence of procedural safeguards.

2. Weak foundations of Aadhaar

Aadhaar is touted as a tool to increase inclusiveness in welfare schemes and improve governance mechanisms, but there is strong evidence from the last decade to suggest that Aadhaar linkage has instead led to exclusion, potential citizen surveillance and profiling, and a range of privacy concerns.[45] A fundamental challenge with Aadhaar enrollment that persists to present day is that it is optional on paper, but it has been thrust upon populations and made mandatory in practice across public and private sectors through the years.[46] We trace some key pitfalls of the Aadhaar project across these themes.

Aadhaar in public and private

In *Puttaswamy (Constitutionality of Aadhaar Act)* judgement (**"Puttaswamy-II**"), the Supreme Court struck down Section 57 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("**Aadhaar Act**"), thus holding that private companies could not require Indians to provide their Aadhaar numbers for the provision of services. Then on April 20, 2023, the union government released draft amendments to the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020 ("**Aadhaar Amendment Rules, 2023**") for public consultation. The amendments proposed changes to Rule 3, which relates to 'Purposes for Aadhaar authentication', to include "*promoting ease of living of residents and enabling better access to services for them*" as a prescribed purpose, and to Rule 4, allowing any non-government entity, that seeks to be able to perform Aadhaar authentication, to submit a proposal to the "*concerned government Ministry or Department*" justifying that their intended purpose falls under Rule 3 of the Aadhaar Amendment Rules, 2023.

---

[44] In January 2023, a constitutional bench of the Supreme Court in *Kaushal Kishor v. State of Uttar Pradesh [2023 4 SCC 1]* applied fundamental rights horizontally on a case-by-case basis, considering the nature of the right violated and the extent of the violator's obligation.# Consequently, it affirmed that "*a fundamental right under Article 19/21 can be enforced even against persons other than the State or its instrumentalities*", which applies *para materia* to the right to privacy.

[45] "Myths." Rethink Aadhaar. Accessed May 30, 2024. https://rethinkaadhaar.in/myths.
See also: Khera, Reetika. "Aadhaar Failures and Food Services Welfare." EPW Engage, April 5, 2019. Accessed May 30, 2024. https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare.

[46] Khera, Reetika**.** "Impact of Aadhaar on Welfare Programmes." EPW Engage, January 20, 2024. Accessed May 30, 2024. https://www.epw.in/journal/2017/50/special-articles/impact-aadhaar-welfare-programmes.html.

The Aadhaar Amendment Rules, 2023 present an indirect attempt at bypassing prohibitions on rulemaking as per *Puttaswamy-II*, defining purposes of Aadhaar which exceeds the scope of the parent legislation, and failing the proportionality tests laid down in *Puttaswamy-I*.[47] It was shortly reported that Google Pay, WeWork and LinkedIn initiated the process of verification via Aadhaar under the amendment.[48] This feeds into concerns on whether other services/platforms will follow the cue and mandate Aadhaar verification for their usage. This is further a dangerous precedent to set in context of the existing unaddressed vulnerabilities in the Aadhaar database and its corresponding implications for data protection, which we cover in detail in later sections.[49]

In *Puttaswamy-II*, the Supreme Court upheld the constitutionality of Aadhaar linkages for welfare services but clearly stated that alternate and viable means of identification like Passport, Driving licence, etc. should suffice for identification purposes, which is also reflected in Section 7 of the Aadhaar Act. On December 14, 2022, the Tamil Nadu government announced that all individuals eligible for benefits under various government schemes, except for minor children, must provide proof of possession of an Aadhaar number or undergo Aadhaar identification—making Aadhaar authentication the only means through which the benefits may be availed.[50] During the COVID-19 pandemic, the union government promoted the adoption of Aadhaar by design—in a manner that made it the "preferred" means of verification and authentication for various government programmes, including for accessing vaccines, social security under NREGA, and benefits under a maternal and child nutrition scheme, POSHAN.[51]

Several Ministries have maintained that Aadhaar authentication is "voluntary", but is necessary if a citizen wishes to access a public service online.[52] The Ministry of Road Transport, under the Aadhaar Amendment Rules, 2023, has requested the use of Aadhaar authentication for online applications for

---

[47] Rohin Garg, "Bad Rules for Good Governance." Internet Freedom Foundation, April 27, 2021. Accessed May 29, 2024. https://internetfreedom.in/bad-rules-for-good-governance/.

[48] WeWork India (@WeWorkIndia). August 8, 2023. https://x.com/WeWorkIndia/status/1688819060388319232;
See also: Aneeka Chatterjee. "GPay introduces UPI verification through Aadhaar." The Hindu Business Line, June 8, 2023. Accessed May 28, 2024.
https://www.thehindubusinessline.com/money-and-banking/gpay-introduces-upi-verification-through-aadhaar/article66942158.ece.

[49] Srinivas Kodali. "UIDAI's Defensive Stance on Aadhaar Security Breaches Isn't Helping Anybody but the Government." The Wire, January 5, 2018. Accessed May 28, 2024. https://thewire.in/politics/uidai-aadhaar-security-breach.

[50] "Appointment to the Treasuries & Accounts Department as Sub Authentication User Agency (Sub-AUA) with the Tamil Nadu e-Governance Agency (TNeGA) under the regulation 15 of Aadhaar Regulations (Authentication) 2016." Finance Department, Government of Tamil Nadu, December 14, 2022. Accessed May 29, 2024.
http://www.stationeryprinting.tn.gov.in/gazette/2022/50_II_1.pdf. See also : "Tamil Nadu government makes Aadhaar a must for all of its schemes." The Hindu, December 18, 2022. Accessed May 29, 2024.
https://www.thehindu.com/news/national/tamil-nadu/tamil-nadu-government-makes-aadhaar-a-must-for-all-of-its-schemes/article66278627.ece.

[51] Anuj Srivas. "The Government's Playbook for 'Mandatory' Aadhaar is Slowly Becoming Clear." The Wire, January 6, 2017. Accessed May 28, 2024. https://thewire.in/government/governments-playbook-mandatory-aadhaar-slowly-becoming-clear.
See also: Abantika Ghosh. "Used Aadhaar for COVID vaccine? Modi govt created your digital health ID without asking you." The Print, October 1, 2021. Accessed May 28, 2024.
https://theprint.in/health/used-aadhaar-for-COVID-vaccine-modi-govt-created-your-digital-health-id-without-asking-you/742958/. See also: Thomson Reuters Foundation. "Children without Aadhaar shut out of school." Deccan Herald, July 29, 2022. Accessed May 28, 2024. https://www.deccanherald.com/national/children-without-aadhaar-shut-out-of-school-1131133.html.

[52] "Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020." Ministry of Electronics and Information Technology, August 5, 2020. Accessed May 28, 2024.
https://www.uidai.gov.in//images/Aadhaar_Authentication_for_Good_Governance_Rules_2020.pdf.

licences learners and other associated services.[53] Aadhaar has become *de facto* mandatory to access public services online, thus creating a barrier to access for those who do not wish to furnish their details or enrol in the project. An inefficient mandatory Aadhaar-based Payment System ("**ABPS**") under NREGA has made a large fraction of beneficiaries fall through the cracks.[54,55] The Election Laws (Amendment) Act, 2021 pushes to link existing Voter ID cards of citizens with their Aadhaar numbers.[56] IFF, along with other civil society groups, have maintained that linking Voter-ID with Aadhaar will gravely violate citizens' right to privacy by enabling voter profiling and linkage of data sets.[57] This plan has since been on hold and no such linking has reportedly taken place ahead of India's 2024 Lok Sabha Election.[58]

Vulnerabilities of Aadhaar data

There is a rich and demonstrated history of Aadhaar-related data leaks in India, which we have annexed to this submission.[59] The non-exhaustive list charting ten prominent examples in the last five years alludes to the lack of robust security measures at various government machineries which record Aadhaar information, and within the central Aadhaar database itself. Some of the instances enumerated may not be direct breaches of the central Unique Identification Authority of India (**"UIDAI"**) database, but nonetheless represent a worrying lapse in responsibility from the regulator.

Deferring accountability to state-owned state government-level Aadhaar data repositories, called State Resident Data Hubs ("**SRDH**"), as UIDAI has previously done, is not an appropriate response to Aadhaar data leaks.[60] At the time of Aadhaar roll-out, SRDHs were established as duplicates of the central database, with technical support from the central regulator, UIDAI.[61] Experts believe that the very constitution of SRDHs is a privacy risk and *ultra vires* the Aadhaar Act, as it stores details of one's identity cards and Aadhaar data without privacy or data use policies in place, and can allow third parties

---

[53] "Notification S.O. 1026(E)." Ministry of Road Transport and Highways, March 03, 2021. Accessed May 29, 2024. https://www.medianama.com/wp-content/uploads/2021/03/225616.pdf.

[54] "Will penalise states not MGNREGA workers if not linked with Aadhaar-based payment system: Minister." CNBC TV18, January 02, 2024. Accessed May 28, 2024. https://www.cnbctv18.com/economy/mgnrega-scheme-workers-giriraj-singh-states-aadhar-18701161.htm.

[55] Sravasti Dasgupta. "MGNREGA: After Pushback on Aadhaar-Based Pay, Govt Defensive, Says May Consider Exemptions Case-by-Case." The Wire, January 02, 2024. Accessed May 29, 2024. https://thewire.in/labour/union-government-may-consider-case-by-case-exemptions-to-abps-mgnregs.

[56] "The Election Laws (Amendment) Bill, 2021." Lok Sabha. Accessed May 29, 2024. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/162_2021_LS_Eng.pdf; See also: "The Election Laws (Amendment) Bill, 2021." PRS Legislative Research. Accessed May 29, 2024. https://prsindia.org/billtrack/the-election-laws-amendment-bill-2021/.

[57] Anushka Jain. "How to protect yourself from coercive Aadhar- Voter ID linking." Internet Freedom Foundation, October 28, 2022. Accessed May 29, 2024. https://internetfreedom.in/how-to-protect-yourself-from-coercive-aadhaar-voter-id-linking/**;** See also: "CCG Open Statement Linking Voter ID & Aadhaar – A Dangerous Move." Constitutional Conduct Group, 2022. Accessed May 30, 2024. https://constitutionalconduct.com/2021/12/29/ccg-open-statement-linking-voter-id-aadhaar-a-dangerous-move/.

[58] "Linking of Aadhaar details with voter ID not yet begun, says govt." Business Standard, December 8, 2023. Accessed May 29, 2024. https://www.business-standard.com/india-news/linking-of-aadhaar-details-with-voter-id-not-yet-begun-says-govt-123120801173_1.html.

[59] See: Annexure 1 to IFF's written contribution to UNHRC.

[60] Sudhakar Reddy. "IT grids Aadhaar data theft case may be the biggest ever in India: Experts." The Times of India, April 15, 2019. Accessed May 30, 2024. https://timesofindia.indiatimes.com/city/hyderabad/it-grids-aadhaar-data-theft-case-may-be-the-biggest-ever-in-india-experts/articleshow/68880147.cms.

[61] "UIDAI, SRDH Adoption Guidelines." Accessed May 29, 2024. https://archive.org/details/SRDHGuidelinesV3, See also: "SRDH Notification." Accessed May 29, 2024. http://degs.org.in/UIDAI.aspx.

to access such sensitive information as well.[62] In fact, SRDH users with administrator privileges have been able to link multiple identity cards like passports and driver's licences to one's Aadhaar, without their consent or knowledge.[63]

Since the beginning, the Aadhaar Project has been plagued with instances of mass exclusion, fraud, leakage, and biometric failure.[64] A number of authorities, including the Comptroller and Auditor General of India, have questioned the sanctity of the Aadhaar Database.[65] Given its risks and problematic roll-out strategies which potentially flout *Puttaswamy* principles, Aadhaar continues to be one of India's most fertile grounds for privacy, data protection, digital exclusion, and cybersecurity-related concerns.

3. An inadequate data protection law

In the introduction and passing of India's umbrella data protection legislation, the DPDPA, 2023, MeitY did not adhere to the Pre-legislative Consultation Policy, 2014 (**"PLCP"**), which obligates the legislative to release a law for public comment before introducing it in the Parliament[66] The contents of the DPDPA, 2023 also raise alarms.[67]

The present Act excludes from its ambit any publicly available personal data, which makes data principles vulnerable to online scraping. It has weak notice requirements for data sharing, storage or transfer, and worryingly imposes duties and penalties on data principles. The Act is replete with vague or indefinite provisions—processing of data without consent is allowed for "*certain legitimate uses*" which are not adequately defined. Cross-border data transfer provisions are vague and only extend to countries not specified in a 'blocklist' which is to be notified later. In many instances in the Act, enforcement is left up to Rules that will be notified later by the union government. Additionally, sweeping exemptions may be awarded to the government and private actors through Rules. The right to information has been diluted by amendments to the RTI Act, 2005. The Act fails to provide safeguards against overbroad surveillance. The Data Protection Board, a statutory body slated to oversee the implementation of the Act, may not be an independent, neutral and impartial body, and is empowered to direct the union government to block access to information in public interest.

---

[62] Aman Sethi. "Why state data hubs pose a risk to Aadhaar security." Hindustan Times, May 13, 2018. Accessed May 30, 2024. https://www.hindustantimes.com/india-news/why-state-data-hubs-pose-a-risk-to-aadhaar-security/story-Klyl3yT5MkFk6Szg2yGg9N.html.

[63] Ibid.

[64] Rachna Khaira. "Aadhaar Operator's Biometrics Stolen & Misused, UIDAI Documents Prove." Huffpost, February 20, 2019. Accessed May 28, 2024. https://www.huffpost.com/archive/in/entry/aadhaar-operators-biometrics-stolen-misused-uidai-documents-prove_in_5c6cf9a4e4b0e2f4d8a0ae2a.

[65] Aashish Aryan. "Explained: The common complaints about Aadhaar, which CAG has now flagged in UIDAI audit." The Indian Express, April 9, 2022. Accessed May 29, 2024. https://indianexpress.com/article/explained/cag-report-uidai-audit-aadhaar-data-7857808/.

[66] Sravasti Dasgupta. "Opposition MPs on Data Protection Bill Panel Refuse to Back 'Report', Accuse Govt of Breaking Rules." The Wire, August 1, 2023. Accessed May 30, 2024. https://thewire.in/government/john-brittas-data-protection-bill-panel-opposition-parliament.

[67] Anushka Jain and Prateek Waghre. "IFF's First Read of the Draft Digital Personal Data Protection Bill 2023." Internet Freedom Foundation, August 3, 2023. Accessed May 29, 2024. https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/.

DPDPA, 2023 has been notified but not implemented. Many of its provisions will be actualised through Rules, which are yet to be released for public scrutiny. Media reports suggest that around the 21 draft Rules will be released soon on a 45-day public consultation—which is highly inadequate and requires reconsideration.[68]

4. Surveillance through CMS

The Centralised Monitoring System ("**CMS**") is an ambitious State e-surveillance system that monitors text messages, social-media engagement, and phone calls on landlines and cell phones, among other communications.[69] Operated by the Department of Telecommunications, CMS purportedly helps the union government 'strengthen the security infrastructure' of the country by automating the process of lawful interception and monitoring of telecommunications.[70] We have deeply analysed the information flow and identified a few key concerns.[71] A wide array of security and intelligence agencies, also exempted under the RTI Act, 2005, are onboarded onto the CMS and have access to this information without adequate safeguards such as transparency into grounds for interception or intercepted data.[72] Concerns about potential privacy violations through such an opaque law enforcement architecture are further exacerbated due to the lack of an active or adequate data protection legislation and also the fact that the CMS framework, at its core, fails to meet *Puttaswamy* thresholds of legality, necessity, proportionality and procedural safeguards.[73]

In India, the Indian Telegraph Act, 1885, deals with interception of calls under Section 5(2), and the IT Act, 2000, deals with interception of data under Section 69—under both laws, only the government, under

---

[68] Aditi Agarwal. "Draft rules under privacy law almost ready: IT minister." Hindustan Times, October 28, 2023. Accessed May 30, 2024. https://www.hindustantimes.com/india-news/draft-rules-under-privacy-law-almost-ready-it-minister-101698431489684.html, See also: "Public notice for the consultation on the draft 'Digital Personal Data Protection Bill, 2022." Ministry of Electronics and Information Technology, November 18, 2022. Accessed May 29, 2024. https://drive.google.com/file/d/1TmwiMv_MSpZnkk-XljdJeln5f4WZcNPc/view.

[69] Anjani Trivedi "In India, PRISM-like Surveillance Slips Under the Radar." Time, June 30, 2013. Accessed May 30, 2024. https://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

[70] CMS aims to remove or bypass the middle man, i.e., telecom service providers ("TSPs"), and allow the law enforcement agency to "tap into communications (of suspected targets) at will without informing TSPs" through a central system.

[71] Anushka Jain. "Watch the Watchmen Series Part 1: The National Intelligence Grid." Internet Freedom Foundation, September 2, 2020. Accessed May 30, 2024. https://static.internetfreedom.in/watch-the-watchmen-part-1-the-national-intelligence-grid/; Anushka Jain. "Watch the Watchmen Series Part 2: The Centralised Monitoring System." Internet Freedom Foundation, September 14, 2020. Accessed May 30, 2024. https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/.

[72] The participating law enforcement agencies of the CMS are: Intelligence Bureau; Central Bureau of Investigation; Directorate of Revenue Intelligence; Research & Analysis Wing; National Investigation Agency; Narcotics Control Bureau; Enforcement Directorate; Central Board of Direct Taxes; Directorate of Signal Intelligence; Commissioner of Police, Delhi. See also: Keerthana Sankaran. "Big Brother is here: Amid snooping row, govt report says monitoring system 'practically complete" The New Indian Express, December 24, 2018. Accessed May 31, 2024. https://www.newindianexpress.com/nation/2018/dec/24/big-brother-is-here-amid-snooping-row-govt-report-says-monitoring-system-practically-complete-1915866.html?ref=static.internetfreedom.in; Litton, Addison. "The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression." Washington University Global Studies Law Review, 2015. Accessed May 31, 2024. https://openscholarship.wustl.edu/cgi/viewcontent.cgi.

[73] Anushka Jain. "Watch the Watchmen Series Part 2: The Centralised Monitoring System." Internet Freedom Foundation, September 14, 2020. Accessed May 30, 2024. https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/.

certain circumstances, is permitted to conduct surveillance.[74] However, both these provisions lack procedural safeguards which would ensure that they are used by the government in a justified manner. Thus, the government enacted specific Rules—Rule 419A of Indian Telegraph (Amendment) Rules, 2007 and the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (**"IT Decryption Rules, 2009"**)—under which interception and monitoring orders can only be issued by the Secretary in the Ministry of Home Affairs (**"MHA"**).[75] The CMS framework also flouts these limitations by authorising up to ten agencies for above stated purposes under the IT Act, 2000.[76] The present regulatory environment on surveillance (or the lack thereof) is too feeble to prevent unchecked and invalid interception by government agencies.[77] Notably, key provisions relating to surveillance, which have a long lasting, profound impact on digital rights, have been replicated verbatim from the Telegraph Act, 1885 in the Telecommunications Act, 2023, which will replace the former once operationalised.

V. State of Free Speech in India

1. The right to peaceful protests

Indian citizens have the fundamental right to protest, drawing from the right to freedom of free speech and expression i.e. Article 19(1)(a) and freedom of peaceful assembly i.e. Article 19(1)(b) of the Indian Constitution. While this right is not absolute and can be limited by reasonable restrictions, such restrictions must be necessary, proportionate, and follow procedure established by law. Over the past few years, the Indian government has routinely adopted means of digital repression, such as internet shutdowns and disproportionate censorship, in response to protests. The use of such often unnecessary and disproportionate tools undermines the free flow of information related to peaceful assembly and the fundamental right to assembly.

India-specific research conducted by Jan Rydzak suggests that internet shutdowns are ineffective in pacifying protests, and have the unintended consequence of incentivising violent forms of collective action which require less communication.[78] Lack of access to internet services inhibits individuals' ability to fact-check information and document human rights abuses perpetrated by state actors. To justify internet shutdowns, the government authorities have expressed concerns about the farmers' protests leading to property damage—however, India incurred an economic cost of $585.4 million due to internet

---

[74] Jayant Sriram. "What are the surveillance laws in India?" The Hindu, November 17, 2019. Accessed May 31, 2024. https://www.thehindu.com/news/national/what-are-the-surveillance-laws-in-india/article29993602.ece.

[75] "The Indian Telegraph (Amendment) Rules, 2007." Ministry of Communications and Information Technology. Accessed May 30, 2024. https://dot.gov.in/sites/default/files/march2007.pdf.
See also: "The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009." Ministry of Communications and Information Technology. Accessed May 30, 2024. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf.

[76] Tathagata Satpathy, Karnika Seth and Anita Gurumurthy. "Are India's laws on surveillance a threat to privacy?" The Hindu, December 28, 2018. Accessed May 31, 2024. https://www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25844250.ece.

[77] Anjani Trivedi "In India, PRISM-like Surveillance Slips Under the Radar." Time, June 30, 2013. Accessed May 30, 2024. https://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

[78] Rydzak, J. "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." SSRN, February 7, 2019. Accessed May 31, 2024. https://papers.ssrn.com/sol3/papers.cfm.

shutdown extending up to 7,812 hours in the year 2023.[79] Shutdowns disrupt the ability of journalists to provide real time updates about the protests and the ability of farmers to present their version of events through social media. Farmers also found it hard to get supplies in absence of internet and SMS services, impacting their right to life.

Digital repression to suppress dissent

In February 2021, the union government reportedly blocked ~2000 X accounts, belonging to a diverse group of entities such as news media organisations, politicians, activists, and farmers groups.[80] The rationale reportedly was that these accounts had been making provocative tweets about the farmer protests and using a specific hashtag.[81] This was not substantiated as the takedown orders directing such censorship were not made public. IFF wrote to MeitY requesting that the accounts be restored, and that the blocking orders be disclosed.[82] MeitY responded that their actions were "authorised by law", and that they are not required to disclose the blocking orders.[83]

In February 2024, the state government of Haryana issued internet shutdown orders amidst calls for protest by the Samyukta Kisan Morcha and Kisan Mazdoor Morcha, citing "*spread of misinformation and rumours through various social media platforms*" and "*for facilitation and mobilisations of mobs and agitators and demonstrators who can cause serious loss of life and damage to public and private properties*".[84] The cited reasons were vague and the order failed to cite any actual evidence to support the shutdown. X accounts documenting protests and alleged human rights violations during the 2024 farmers protest were reportedly also being withheld in India, purportedly due to legal demands under the IT Act, 2000.

The union government suspended internet services across multiple states in response to the protests against the Citizenship (Amendment) Act, 2019 and National Register of Citizens ("**CAA/NRC**") in December 2019.[85] The Government of Rajasthan suspended internet services in response to protests

[79] Samuel Woodhams and Simon Migliano. "Cost of Internet Shutdowns." Top10VPN, May 8, 2024. Accessed June 1, 2024. https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

[80] Rohin Garg. "Government Censorship and the dire need for transparency." Internet Freedom Foundation, February 8, 2021. Accessed May 29, 2024. https://internetfreedom.in/government-censorship-and-the-dire-need-for-transparency/.
See also: Anumeha Chaturvedi and Anandita Singh. "Farmer Protests: Govt Sends Fresh Notice to Twitter on Accounts Flagged." The Economic Times, February 8, 2021. Accessed June 1, 2024. https://economictimes.indiatimes.com/tech/technology/farmer-protests-govt-sends-fresh-notice-to-twitter-on-accounts-flagged/articleshow/80738857.cms.

[81] "Twitter Withheld Caravan's Tweet on Kisan Ekta Morcha." The Wire, February 1, 2021. Accessed June 1, 2024. https://thewire.in/rights/twitter-withheld-caravan-kisan-ekta-morcha.

[82] Rohin Garg. "Government Censorship and the dire need for transparency." Internet Freedom Foundation, February 8, 2021. Accessed May 29, 2024. https://static.internetfreedom.in/government-censorship-and-the-dire-need-for-transparency/.

[83] "Reply of MeitY to representation sent by IFF pertaining to secretive and disproportionate directions issued to Twitter under Section 69A of the Information Technology Act, 2000." Internet Freedom Foundation, April 26, 2021. Accessed May 29, 2024. https://drive.google.com/file/d/1H2xcqeTVYnROlIm7AzGiiAG7YwvIsa7w/view.

[84] "Statement: The ongoing internet shutdowns in the states of Haryana and Rajasthan, & online censorship in response to Farmers Protest." Internet Freedom Foundation, February 13, 2024. Accessed May 31, 2024. https://internetfreedom.in/the-ongoing-internet-shutdowns-in-the-states-of-haryana-rajasthan-online-censorship-in-response-to-farmers-protest/.

[85] "CAA internet shutdowns: Violation of basic rights or extension of law enforcement measure." The Print Team December 20, 2019. Accessed May 31, 2024. https://theprint.in/talk-point/caa-internet-shutdowns-violation-of-basic-rights-or-extension-of-law-enforcement-measures/338536/.

against the lack of recruitment of members of the tribunal community for teaching posts.[86] Reliance on such disproportionate, unnecessary, and suppressive tools, that often are shrouded in secrecy, runs counter to the government's obligations not to restrict peaceful assemblies unnecessarily or disproportionately.[87]

Protest surveillance

In December 2019, the Delhi police force used FRT to profile people attending the Prime Minister's Ramlila Maidan rally by matching them with facial datasets collected from protests.[88] Noting that such use can open floodgates and set dangerous precedents on the free and unchecked use of surveillance technologies to stifle the freedom of speech and expression, we promptly sent a legal notice to the Delhi Police, asking them to halt the use of FRT altogether.[89] However, reports started emerging in 2020 on the continued and rampant use of facial recognition by the Delhi Police during the highly mobilised and contested protests against CAA/NRC.[90] On March 11, 2020, the Union Minister of Home Affairs, while replying to a short duration discussion on the Delhi riots in the Lok Sabha, stated that, "*police have identified 1,100 people through facial recognition technology*".[91] FRT was reportedly used to identify individuals who were present during the 2021 'tractor rally violence' incident and Republic Day protests at the Red Fort in New Delhi, with one person being arrested using this technology.[92]

In February 2024, Haryana police deployed unmanned aerial vehicles ("**UAV**"s) such as drones to drop tear gas shells on farmers protesting near the Shambhu Border as part of the Delhi Chalo march, marking the first time that any Indian police force has used drones to silence protesters in this manner.[93] It was not confirmed at the time whether the drones also possessed facial detection or recognition technologies, but it was later reported that Haryana police began cancelling passports and visas of farmers identified through drone and CCTV cameras to be "causing disturbances" during the farmers' protests. As of May 2024, we do not have any transparency on the make and model of these drones, the kind of equipment

[86] Krishnesh Bapat. "[Revealed] Udaipur Internet Shutdown Orders: Cut, Copy and Paste." Internet Freedom Foundation, November 1, 2021. Accessed May 31, 2024. https://internetfreedom.in/revealed-udaipur-internet-shutdown-orders-cut-copy-paste/.

[87] "India: Right to Peaceful Protest Under Threat Due to Mounting Restrictions and Escalating Crackdown on Farmers' March." Amnesty International, February 14, 2024. Accessed May 31, 2024. https://www.amnesty.org/en/latest/news/2024/02/india-right-to-peaceful-protest-under-threat-due-to-mounting-restrictions-and-escalating-crackdown-on-farmers-march/.

[88] Jay Mazoomdaar. "Delhi Police film protests, run its images through face recognition software to screen crowd." The Indian Express, December 28, 2019. Accessed June 1, 2024. https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/.

[89] Apar Gupta. "The Delhi Police must stop it's facial recognition system." Internet Freedom Foundation, December 29, 2019. Accessed May 31, 2024. https://static.internetfreedom.in/we-demand-the-delhi-police-stop-its-facial-recognition-system/.

[90] "Delhi, UP Police Use Facial Recognition Tech at Anti-CAA Protests, Others May Soon Catch Up." India Today, February 18, 2020. Accessed May 31, 2024. https://www.indiatoday.in/india/story/delhi-up-police-use-facial-recognition-tech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18.

[91] "1,100 rioters identified using facial recognition technology: Amit Shah." The Hindu, March 12, 2020. Accessed May 30, 2024. https://www.thehindu.com/news/cities/Delhi/1100-rioters-identified-using-facial-recognition-technology-amit-shah/article31044548.ece.

[92] "Delhi Police Arrests Man Who Instigated R-Day Tractor Rally Violence." India.com, February 8, 2021. Accessed May 30, 2024. https://www.india.com/news/india/delhi-police-arrests-man-who-instigated-r-day-tractor-rally-violence-4405095/

[93] Vijaita Singh. "Haryana Police is first force to use drones for tear gas." The Hindu, February 13, 2024. Accessed May 30, 2024. https://www.thehindu.com/news/national/haryana-police-is-first-force-to-use-drones-for-tear-gas/article67842865.ece.

used, or how police officials are able to use them to identify farmers and even "*check movement on the left and right side of the bridges and drop shells accordingly.*"[94] The lack of information is a cause for concern because globally, drones used by law enforcement agencies to stifle protests usually come equipped with advanced surveillance technologies like FRT cameras, microphones, speakers, or communications interception tools.[95]

India is moving towards deploying modern and extremely dangerous surveillance tools during protests in the name of law enforcement. Surveillance of protesters and collection of data about their faces, location, or movement can severely jeopardise their fundamental rights to privacy and to freedom of speech and movement, as enshrined in Articles 21, 19(1)(e) and 19(1)(d) of the Indian Constitution respectively. Moreover, Indian police forces use drones and CCTV cameras in a regulatory vacuum.

UAVs, including drones, are used by law enforcement agencies in the absence of an adequate legal framework to prohibit their misuse or arbitrary deployment. Drone Rules, 2021 currently regulate UAVs in India, but merely create a licensing regime with the objective of regulating private entities that wish to operate UAVs in specified flying zones for research and development purposes.[96] They do not govern or prescribe any standards or limitations for drone use by government agencies. This is worrying because the past year has seen a spike in demand for drones by Indian law enforcement agencies for policing, surveillance, security, or maintaining law and order.[97] Additionally, the use of real-time or reverse FRT, and even CCTVs, happens in the absence of similar SOPs, guidelines, and safeguards. Identification through FRT and CCTV cameras has been known to be inaccurate and based on existing biases, which may unfairly misidentify and implicate any individual without many legal safeguards available to them.[98] Further, there is no transparency on the personal and non-personal data these law enforcement agencies collect through surveillance tools, how they use or process it, who they share it with, and so on. Without clear and adequate legal safeguards or procedures that put necessary limitations on executive power and allow citizens to claim protection against misuse and misidentification, use of surveillance tools by the police during protests remains arbitrary and potentially unconstitutional.

2. Internet shutdowns

Statutory basis for internet shutdowns in India

Section 5(2) of the Indian Telegraph Act, 1885 allows the union or state government to restrict or temporarily suspend internet and telecom services in case of a "public emergency" or "in the interest of public safety" and if it is "necessary" to do so in the interest of the sovereignty and integrity of India, the

[94] Bhavey Nagpal. "How drones came in handy for Haryana cops." Hindustan Times, February 14, 2024. Accessed May 31, 2024. https://www.hindustantimes.com/cities/chandigarh-news/how-drones-came-in-handy-for-haryana-cops-101707845887551.html.
[95] "How police drones technology can be used at a protest." Privacy International, May 5, 2021. Accessed May 31, 2024. https://privacyinternational.org/explainer/4498/how-police-drones-technology-can-be-used-protest.
[96] "Drone Rules, 2021." Ministry of Civil Aviation, July 15, 2021. Accessed May 30, 2024. https://egazette.gov.in/WriteReadData/2021/229221.pdf.
[97] Vallari Sanzgiri. "Why Is No One Asking About The Growing Use Of Drones By Police In India?" MediaNama, April 06, 2023. Accessed May 30, 2024. https://www.medianama.com/2023/04/223-growing-use-drones-police/.
[98] "Status of Policing in India Report 2023." Common Cause, 2023, Accessed May 30, 2024. https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf.

security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence. The procedure to suspend telecom/internet services is delineated in the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (**"Suspension Rules"**). Rule 2(5) of the Suspension Rules requires a three-member Review Committee consisting only of bureaucrats to examine the legality of internet suspension orders. The Review Committee does not have the power to strike down or set aside illegal suspension orders.It is merely supposed to "record its findings".

Anuradha Bhasin v. Union of India [AIR 2020 SC 1308] held that the suspension of telecom services, including internet services, constitutes a "drastic measure" that the State may consider only if it is "necessary" and "unavoidable," and after evaluating the availability of less intrusive alternatives. Second, it endorsed a proportionality standard directed by union and state governments to ensure that internet shutdowns do not violate constitutional rights, mandating that suspension orders must be lawful, necessary and proportionate. Third, noting the flaws in the Suspension Rules, the Supreme Court read in the requirement that the telecom/internet suspension orders must be published/notified through "a suitable mechanism" so that they may be assailed before a suitable forum. Fourth, The Court held that the nature of restrictions contemplated in the Suspension Rules is "temporary" in nature and they must not extend beyond the necessary duration. The Supreme Court also noted the exceptional nature of internet shutdowns in *Foundation of Media Professionals v. Union Territory of Jammu & Kashmir [(2020) 5 SCC 746]*, where it held that internet suspension orders must be territorially limited and cannot be permanent.[99]

In November 2020, the Suspension Rules were amended to include Rule 2A, which limits internet shutdown orders to a maximum of 15 days. This amendment is a missed opportunity for broader reform as it fails to incorporate the Supreme Court's directives in *Anuradha Bhasin* which require proactive publication of shutdown orders and periodic review by the Review Committee.

State authorities often resort to Section 144 of the Code of Criminal Procedure, enabling district magistrates to take preventive measures against imminent threats to public order, including suspending internet services. These orders are often issued without publication, lacking accountability and oversight. Magistrates can issue such orders *ex parte,* with no review mechanism in place.

Internet shutdowns in practice

Despite the law permitting suspension of internet services only in exceptional circumstances, internet shutdowns are commonplace in India, and are even deployed to prevent cheating in exams or in response to protests/strikes.[100] A report titled "No Internet Means No Work, No Pay, No Food —Internet Shutdowns Deny Access to Basic Rights in "Digital India" published by IFF and Human Rights Watch

[99] Foundation of Media Professionals v. Union Territory of Jammu & Kashmir, (2020) 5 SCC 746.
[100] Anandita Mishra. "The internet cannot be suspended in entire districts to prevent cheating in exams." Internet Freedom Foundation, September 27, 2021. Accessed May 30, 2024.
https://internetfreedom.in/the-internet-cannot-be-suspended-in-entire-districts-to-prevent-cheating-in-exams-iff-writes-to-the-rajasthan-government/.
See also: Aihik Sur. "Internet Suspended In Arunachal Pradesh In Response To A Bandh Called By A Political Outfit." Medianama, January 13, 2022. Accessed May 31, 2024.
https://www.medianama.com/2022/01/223-internet-shutdown-arunachal-pradesh/.

examines the law which permits the executive to unilaterally suspend internet services without any oversight.[101] As per the report, the Supreme Court's directions in *Anuradha Bhasin* are continuously ignored.[102] The report demonstrates this by listing the 127 instances of internet shutdowns in the three years between the judgement and December 31, 2022. Out of 28 Indian states, 18 states shut down the internet at least once during this period, and 11 of them did not publish shutdown orders. In 2023 and 2024, state governments continued to impose internet shutdowns to address communal violence, quell protests, prevent cheating, regulate information disorder, and control law and order situations.[103] One notable instance was in Manipur, which experienced an indefinite internet shutdown spanning over 200 days. This shutdown was maintained through a series of templated orders. In 2024, the union government also imposed internet shutdowns to quell farmers' protests.

Challenge to the validity of Suspension Rules

The validity of the Suspension Rules has been challenged before the Gauhati High Court.[104] These Rules allow blanket internet suspension orders, failing to distinguish between lawful speech (discussion, debate, advocacy) and unlawful speech (incitement to violence). Additionally, the Rules enable a secretary-level officer to suspend internet services without judicial oversight. Despite studies indicating that internet suspensions do not improve law and order, the Rules permit such measures, potentially incentivising violent actions over peaceful protests.

3. Digital censorship

The Supreme Court has time and again held that the constitutionally guaranteed right to freedom of speech and expression can only be restricted based on specifically enumerated grounds under Article 19(2) of the Constitution. India has a declaration to Article 19(3) of the ICCPR, stating that the provisions of the said article shall be applied in conformity with the provisions of Article 19 of the Constitution of India.

---

[101] Krishnesh Bapat and Tanmay Singh. "Our report with HRW on internet Shutdowns demonstrates a disproportionate impact on communities dependent on welfare." Internet Freedom Foundation, June 21, 2023. Accessed May 31, 2024. https://internetfreedom.in/our-report-with-hrw-on-internet-shutdowns-demonstrates-a-disproportionate-impact-on-communities-dependent-on-welfare/.

[102] Anuradha Bhasin v. Union of India, AIR 2020 SC 1308.

[103] Sarasvati NT. "Rajasthan Govt Orders Internet Shutdown During RPSC Exam to Prevent Cheating." MediaNama, January 8, 2024. Accessed May 30, 2024. https://www.medianama.com/2024/01/223-rajasthan-govt-internet-shutdown-rpsc-exam-cheating/#:~:text=In%20September%202022%2C%20the%20Supreme,in%20five%20states%2C%20including%20Rajasthan.
See also: Dev Raj. "Bihar Government Suspends Internet Service in Darbhanga for 72 Hours After Violence." The Telegraph India, July 28, 2023. Accessed May 31, 2024. https://www.telegraphindia.com/india/bihar-government-suspends-internet-service-in-darbhanga-for-72-hours-after-violence/cid/1954948.
See also: Sameer Yasir and Suhasini Raj. "India's Internet Shutdowns Are Taking a Heavy Toll in Punjab." The New York Times, March 20, 2023. Accessed May 31, 2024. https://www.nytimes.com/2023/03/20/world/asia/india-punjab-internet-shutdown-amritpal-singh.html.
See also: "Longest Internet Shutdown in 2023 Took Place in Manipur Amidst Human Rights Violations: Report." The Hindu, January 11, 2024. Accessed May 30, 2024. https://www.thehindu.com/sci-tech/technology/longest-internet-shutdown-2023-took-place-manipur-amidst-human-rights-violations-report/article67726259.ece.

[104] Tanmay Singh and Anandita Mishra "Gauhati HC allows IFF's intervention application in petition challenging the constitutionality of internet shutdowns rules." Internet Freedom Foundation, February 1, 2022. Accessed May 31, 2024. https://internetfreedom.in/gauhati-hc-internet-shutdown-rules-update/.

Trends in online content blocking

A study by the Software Freedom Law Center found that 55,580 websites were blocked in India from 2015 to September 2022.[105] The majority of these blockings, 26,447 websites (47.5% of the total), were carried out under Section 69A of the IT Act.

In response to a question asked in the Rajya Sabha, the IT Minister revealed that between 2018 and October 2023, the union government had issued orders to take down 36,838 URLs on social media.[106] Of these, 13,660 URLs related to X were removed. In 2023 (until October), the union government took down 7,502 URLs, which were 168% higher than the 2,799 URLs taken down in 2018. The maximum number of URLs, amounting to 9849, was taken down in 2020.

Year	Facebook	Instagram	X-Corp (Twitter)	YouTube	Others	Total
2018	1555	379	224	161	480	2799
2019	2049	75	1041	409	61	3635
2020	1717	1273	2731	2175	1953	9849
2021	1082	464	2851	1141	580	6118
2022	1750	359	3423	939	464	6935
2023*	2044	473	3390	934	661	7502

*Till October 2023

Image: Statistical information disclosed in response to questions raised in Parliament.

Website blocking

In July 2020, the website of the environmental activism group Fridays for Future India was blocked following a notice from the Delhi Police under Section 79(3)(b) of the IT Act, 2000.[107] The notice was based on a complaint from the Minister of Environment and Forests, regarding "*multiple emails received on his email address with the subject similar to 'EIA 2020*'."[108] The Delhi Police noted that these emails "may disturb the peace and sovereignty of India" and alleged that the Fridays for Future website displayed "*objectionable content and unlawful activities or terrorist acts, which are dangerous for the peace, tranquillity, and sovereignty of India"* and contained *"religious hatred content/material*." In

[105] Software Freedom Law Center. 2022. "Finding 404: A Report on Website Blocking in India." Software Freedom Law Center. Accessed June 4, 2024. https://sflc.in/finding-404-report-website-blocking-india/.
[106] "Centre Blocks 36,838 Social Media Posts in Last Five Years, X Corp Tops the Chart Among Platforms." The Wire, December 9, 2023. Accessed May 31, 2024. https://thewire.in/rights/centre-blocks-36838-social-media-posts-in-last-five-years-x-corp-tops-the-chart-among-platforms.
[107] Devadutta Mukhopadhyay. "Fridays for Future India resists illegal website blocking." Internet Freedom Foundation, July 23, 2020. Accessed May 31, 2024. https://internetfreedom.in/fridays-for-future-representation-to-delhi-police/#:~:text=Tl%3Bdr,on%20the%20Draft%20EIA%20Notification.
[108] Kabir Agarwal. "Fridays for Future Website Blocked in India After UAPA Mentioned in EIA Protest Document." The Wire, July 23, 2020. Accessed May 30, 2024. https://thewire.in/environment/fridays-for-future-website-block-eia-prakash-javadekar-uapa.

February 2022, the website of VideoLAN Client ("**VLC"**) media player was blocked under Section 69A of the IT Act, 2000 for allegedly "*communicating with servers of a previously banned app, Onmyoji Arena, which was transferring sensitive personal data of Indians to a hostile country*."[109] The website was subsequently unblocked.[110]

Social media account blocking

In 2021, during the farmers' protest, multiple tweets, entire hashtags, and entire accounts of media outlets, journalists, activists, and politicians were blocked.[111] Content from filmmakers, politicians, actors, and a state Minister criticising India's handling of the second COVID-19 wave was removed from X and Facebook.[112] Reportedly, the Indian government also requested social media intermediaries to remove content criticising the government's handling of the COVID-19 crisis under the pretext of spreading misinformation.[113]

In April 2023, following a state-wide internet shutdown in Punjab, reportedly over 2000 X accounts were blocked, including those of BBC Punjabi and poet Rupi Kaur.[114] An RTI application requesting a list of blocked accounts was denied, citing national security.[115] In June, 2023 accounts of local groups in Manipur were reportedly withheld 'under a legal demand'. This arbitrary censorship occurred during the

---

[109] Soumyarendra Barik. "VLC Site Ban Data Transfers to Servers in 'Hostile' Country." The Indian Express, October 12, 2022. Accessed May 29, 2024.
https://indianexpress.com/article/technology/vlc-site-ban-data-transfers-to-servers-in-hostile-country-8201259/.
See also: Anandita Mishra. "VideoLAN Issued Legal Notice to DoT and MeitY for Banning Their Website in India." Internet Freedom Foundation, October 4, 2022. Accessed May 29, 2024.
https://internetfreedom.in/videolan-issued-legal-notice-to-dot-and-meity-for-banning-their-website-in-india/.

[110] Anupriya Chatterjee. "VLC unblocked eight months after ban by Central Govt, reasons for ban still unclear." The Print, November 14, 2022. Accessed May 30, 2024.
https://theprint.in/tech/vlc-unblocked-eight-months-after-ban-by-central-govt-reasons-for-ban-still-unclear/1216216.

[111] Anuj Srivas. "Farmers that Twitter Blocked, Government Order List." The Wire, February 11,2021. Accessed May 30, 2024.
https://thewire.in/tech/farmers-that-twitter-blocked-government-order-list.
See also: Billy Perrigo. "India's Farmers' Protests Become the Biggest in History — And That's Exactly What Modi Wants." Time, February 1, 2021. Accessed May 30, 2024. https://time.com/5935003/india-farmers-protests-twitter/. See also: "Twitter restores several accounts it had withheld over farmer protest tweets." The Hindu, February 3, 2021.
https://www.thehindu.com/news/national/twitter-restores-several-accounts-it-had-withheld-over-farmer-protest-tweets/article33735013.ece

[112] Shirin Ghaffary."India's government is using the pandemic to make huge Facebook and Twitter censorship demands." Vox, May 1, 2021. Accessed May 30, 2024.
https://www.vox.com/recode/22410931/india-pandemic-facebook-twitter-free-speech-modi-COVID-19-censorship-free-speech-takedown.

[113] Newley Purnell. "India Accused of Censorship for Blocking Social Media Criticism Amid Covid Surge." The Wall Street Journal, April 26, 2021. Accessed May 29, 2024.
https://www.wsj.com/articles/india-accused-of-censorship-for-blocking-social-media-criticism-amid-COVID-surge-11619435006
.
See also: "India's removal of tweets critical of COVID response 'dangerous'." Al Jazeera, April 26, 2021. Accessed May 29, 2024.
https://www.aljazeera.com/news/2021/4/26/indias-removal-of-tweets-critical-of-COVID-response-dangerous.

[114] Yashraj Sharma. "Twitter accused of censorship in India as it blocks Modi critics, Elon Musk." The Guardian, April 5, 2023. Accessed May 29, 2024.
https://www.theguardian.com/world/2023/apr/05/twitter-accused-of-censorship-in-india-as-it-blocks-modi-critics-elon-musk.

[115] "MEITY denies information of blocked Twitter accounts in the aftermath of internet shutdown in Punjab." Internet Freedom Foundation, May 5, 2023. Accessed May 29, 2024.
https://internetfreedom.in/top-secret-meity-denies-information-of-blocked-twitter-accounts-in-the-aftermath-of-internet-shutdown-in-punjab-whattheblock/.

state-wide internet shutdown in the state.[116] In 2023, the Facebook and X accounts of the independent news media website "The Kashmir Walla" were blocked.[117] In January 2024, the X account and website of the independent research initiative Hindutva Watch, which documents hate crimes against minority communities, was blocked.[118] The website of the research collective 'India Hate Lab' was also blocked. In 2024, the X and YouTube accounts of reporters, independent news media organisations, influencers, and farmers' unionists were taken down.[119]

X challenged the account takedowns following the 2021 farmers' protest before the Karnataka High Court, marking the first recorded instance of an intermediary challenging takedown orders. Non-compliance with takedown notifications government notifications can result in the loss of safe harbour protections which could result in fines and/or penal consequences. The Karnataka High Court dismissed this challenge and imposed costs of Rs. 50 lakhs on X.[120]

Contradicting settled judicial precedent, the Karnataka High Court held that the observations in *Shreya Singhal* do not mandate providing prior notice and hearing to originators, and that reasons for blocking recorded in writing may not need to be conveyed to the user. Without procedural safeguards, restrictions on free speech can be imposed without oversight or recourse for affected entities to challenge them.[121]Additionally, while acknowledging that blocking orders affect users' rights, the Karnataka High Court held that the State could choose to hear users and that issuance of notice under Rule 8 was not mandatory. The Court also held that claims of originators whose tweets or accounts were blocked could

---

[116] Alka Jain. "Act of Censorship: Twitter account of Manipur's tribal forum blocked in India." Livemint, June 18, 2023. Accessed May 29, 2024. https://www.livemint.com/news/india/act-of-censorship-twitter-account-of-manipurs-tribal-forum-blocked-in-india-manipur-news-11687049402635.html.

[117] "India blocks independent news outlet The Kashmir Walla." Al Jazeera, August 21, 2023. Accessed May 28, 2024. https://www.aljazeera.com/news/2023/8/21/india-blocks-independent-news-outlet-the-kashmir-wallahttps://w.
See also: "India Blocks The Kashmir Walla Website and Social Media Accounts." Committee to Protect Journalists, August 21, 2023. Accessed May 28, 2024. https://cpj.org/2023/08/india-blocks-the-kashmir-walla-website-and-social-media-accounts/.

[118] Vittoria Elliott. "India's Election Commission Is Cracking Down on a Right-Wing Website." Wired, February 12, 2024. Accessed May 29, 2024. https://www.wired.com/story/india-elections-right-wing-website-ban/.
See also: "Delhi HC issues notice on Hindutva Watch's petition challenging the blocking of their entire Twitter account." Internet Freedom Foundation, May 2, 2024. Accessed May 29, 2024. https://internetfreedom.in/delhi-hc-issues-notice-on-hindutva-watchs-petition-challenging-the-blocking-of-their-entire-x-twitter-account-2/.

[119] "India's demand to block accounts amid farmers' stir curtails free speech." Al Jazeera, February 22, 2024. Accessed May 28, 2024. https://www.aljazeera.com/news/2024/2/22/indias-demand-to-block-accounts-amid-farmers-stir-curtails-free-speech-x.
See also: Aliza Noor. "Inside Hundreds of Social Media Accounts of Farmers, Dalit, Tribal Activists Withheld, Blocked." The Quint, February 23, 2024. Accessed May 28, 2024. https://www.thequint.com/news/india/inside-hundreds-of-social-media-accounts-farmers-dalit-tribal-activists-withheld-blocked.
See also: Geetha Pillai. "Activists, Journalists Challenge Centre Govt's Twitter Account Censorship, Vow to Seek Supreme Court Intervention." The Mooknayak, February 23, 2024. Accessed May 28, 2024. https://en.themooknayak.com/india/activists-journalists-challenge-centre-govts-x-account-censorship-vow-to-seek-supreme-court-intervention.

[120] "Karnataka High Court Issues Notice On Plea Challenging Twitter Blocking Orders By Ministry Of Electronics & Information Technology." LiveLaw, June 30, 2023. Accessed May 29, 2024. https://www.livelaw.in/top-stories/karnataka-high-court-twitter-blocking-orders-ministry-electronics-information-technology-case-231544.

[121] Radhika Roy and Gayatri Malhotra. "A Case of Unchecked Power to Restrict Online Free Speech." The Hindu, July 3, 2023. Accessed May 29, 2024. https://www.thehindu.com/opinion/lead/a-case-of-unchecked-power-to-restrict-online-free-speech/article67034902.ece.

not be represented by X, and that none of the affected originators had approached the High Court. This is an incorrect claim, as a user of X whose account was blocked filed an intervention application in the X challenge, and the same was withdrawn after the Court indicated that heavy cost could be imposed on the intervenor.[122]

Reasonable restrictions on the fundamental right to freedom of speech may only be imposed based on the eight specifically enumerated grounds under Article 19(2) of the Constitution. The Supreme Court, in *Shreya Singhal*, clarified that blocking under Section 69A of the IT Act and the 2009 Blocking Rules must adhere strictly to these grounds. Notably, the scope of Section 69A is narrower than Article 19(2). However, the Karnataka High Court's judgement, which reproduces portions of certain blocking orders, reveals that one reason cited was the potential for the content to spread "fake news" and "misinformation," potentially disturbing "public order" and threatening the "security of the State". "Misinformation" and "fake news" are not grounds for restricting free speech under Article 19(2) and Section 69A. The Supreme Court has consistently held that, for speech to be prejudicial to the maintenance of public order, there must be a direct link between the speech and the potential threat to public order.[123]

Existing online censorship practice falls afoul of prevailing legal norms

While undertaking online content removal under Section 69A of the IT Act and the 2009 Blocking Rules , MeitY rarely adheres to procedural safeguards specified in the 2009 Blocking Rules and the directives of the Supreme Court in *Shreya Singhal*.[124] Originators of online content are scarcely, if ever provided with notice and hearing prior to blocking and reasoned copies of the blocking order.[125]

Notably, the Court in *Shreya Singhal* saved Section 69A and the 2009 Blocking Rules from being struck down on the express ground it had "sufficient safeguards"[126] including providing a hearing and reasoned blocking order so that aggrieved parties may challenge the reasons provided in the blocking order under Article 226 of the Constitution. MeitY has historically cited the confidentiality requirement under Rule 16

[122] "Court threatens penalty, Aakar withdraws Twitter plea in HC." The Times of India, October 28, 2022. Accessed May 30, 2024. https://timesofindia.indiatimes.com/city/bengaluru/court-threatens-penalty-aakar-withdraws-twitter-plea-in-hc/articleshow/95133248.cms. See also: Krishnesh Bapat."Karnataka HC Refuses to Permit an Impacted User to Intervene in Twitter's Petition Against Censorship Orders." Internet Freedom Foundation, October 27, 2022. Accessed May 30, 2024. https://internetfreedom.in/karnataka-hc-refuses-to-permit-an-impacted-user-to-intervene-in-twitters-petition-against-censorship-orders/.

[123] Superintendent, Central Prison v. Ram Manohar Lohia, (1960) 2 SCR 821; See also: Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574.

[124] Sehgal, Divyansha. Grover, Gurshabad. "Online Censorship: Perspectives from Content Creators and Comparative Law on Section 69A of the Information Technology Act." SSRN, April 13,2023. Accessed May 30, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404965.

[125] Saurav Das. "Takedown of Hate Tracker Highlights Secrecy Around Modi Govt's Internet Censorship Practices." Article 14, February 9, 2023. Accessed May 30, 2024. https://article-14.com/post/takedown-of-hate-tracker-highlights-secrecy-around-modi-govt-s-internet-censorship-practices-65c59c3549d5a; See also: Zafar Aafaq."The near-impossible task of restoring a blocked Twitter handle in India." Scroll.in, May 1, 2023. Accessed May 30, 2024. https://scroll.in/article/1048073/the-near-impossible-task-of-restoring-a-blocked-twitter-handle-in-india

[126] Shreya Singhal v. Union of India, (2015) 5 SCC 1, Paragraph 115.

of the 2009 Blocking Rules to withhold blocking orders from aggrieved persons.[127] Obtaining a copy of the blocking order is a sisyphean process, as aggrieved parties often have to approach writ courts to obtain blocking orders.[128]

Blocking of future speech acts is impermissible under Section 69A of the IT Act as it is backward-looking and linked to existing content "*any information generated, transmitted, received, stored or hosted in any computer resource*". Blocking entire websites/social media accounts/hashtags is forward-looking, restricting both existing and future content based on the presumption that future content will be illegal. This amounts to pre-censorship and leads to permanent exclusion from participating in the marketplace of ideas. Blocking of the entire accounts/hashtag also fails to satisfy the third prong of the proportionality test i.e., the rights-restricting measure must be the least restrictive way of achieving the legitimate goal.

Attack on journalistic expressions and creative freedom

The Broadcasting Services (Regulation) Bill, 2023 (**"Broadcasting Bill"**), which was released for public consultation in 2023 by MIB, extends the MIB's regulatory ambit to any person who broadcasts news and current affairs programs through a digital medium (such as an online paper, news portal, website, social media intermediary, or another similar medium).[129] Every broadcaster covered under MIB's regulatory ambit will be required to comply with a Code prescribed by the union government, failure to do which will lead to monetary penalties or even imprisonment. The application of such ethical codes on broadcasters, whether an OTT platform or a journalist, will have serious consequences for online free speech and artistic creativity.

Violent content, intimate scenes, religiously flavoured content (including satirical, comedic, and factual), politically unpalatable content, and other such "controversial" pieces of content are also under threat of heavy modification and censorship as the Broadcasting Bill imposes stringent rules and codes to Over-The-Top (**"OTT"**) broadcasters. Previous attempts to suggest self-regulation for on-demand video streaming platforms have been viewed with scepticism in light of increasing censorship, both

---

[127] Gautam Bhatia. "The Supreme Court's IT Act Judgment and Secret Blocking." Indian Constitutional Law and Philosophy, March 25, 2015. Accessed May 30, 2024. https://indconlawphil.wordpress.com/2015/03/25/the-supreme-courts-it-act-judgment-and-secret-blocking/; See also: Rohin Garg and Tanmay Singh. "MEITY Response to Representation to unblock Twitter accounts. Confirms orders and denies disclosure." Internet Freedom Foundation, May 10, 2021. Accessed May 30, 2024. https://internetfreedom.in/meity-response-to-representation/.

[128] Amala Dasarathi. "Delhi HC Directs MEITY to Provide a Copy of the Blocking Order and a Post-Decisional Hearing to Mr. Tanul Thakur." Internet Freedom Foundation, May 16, 2022. Accessed May 30, 2024. https://internetfreedom.in/delhi-hc-directs-meity-to-provide-a-copy-of-the-blocking-order-and-a-post-decisional-hearing-to-mr-tanul-thakur-whattheblock/; See also "Delhi HC directs Union of India to file Inter-ministerial Committee's Report rejecting proposal to Unblock 'Dowry Calculator' in a Sealed Cover." Internet Freedom Foundation, October 5, 2023. Accessed May 30, 2024. https://internetfreedom.in/inter-ministerial-committee-rejects-proposal-to-unblock-dowry-calculator/; See also: Abhinav Sekhri. "Why Defending The Retention Of Sedition, Endorsing Govt Censorship Powers Do Not Defy India's Constitution." Article 14, July 10, 2023. Accessed May 30, 2024. https://article-14.com/post/why-defending-the-retention-of-sedition-endorsing-govt-censorship-powers-do-not-defy-india-s-constitution-64ab0ec58c5c7.

[129] "Public Notice for Soliciting Suggestions/ Comments/Inputs/ Views from General Public/ Stakeholders on the Draft Broadcasting Services (Regulation) Bill, 2023." Ministry of Information and Broadcasting, November 10, 2023. Accessed May 31, 2024. https://drive.google.com/file/d/1ROw6fLMir_tXhsHY1cfHcDFvkhSblCmJ/view?usp=sharing&ref=static.internetfreedom.in

self-imposed and through legal requests.[130] The unfortunate consequence of such censorship is a negative impact on the fundamental right to freedom of speech and expression and excessive self-censorship on part of platforms.[131]

4. Deficiencies in the IT Rules

Platforms are governed in India through a network of laws, including three notable amendments to the IT Act, 2000. These are the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**"IT Rules, 2021"**), Amendment Rules, 2022 to the IT Rules, 2021 (**"IT Amendment Rules, 2022"**), and Amendment Rules, 2023 to the IT Rules, 2021 (**"IT Amendment Rules, 2023"**). We chart their regulatory mechanisms below.

IT Rules, 2021

The IT Rules, 2021, whose legality is contentious, undermines the fundamental right to freedom of speech and expression and privacy for millions of internet users in India and have been unequivocally criticised by experts, civil society, digital rights groups, industry bodies, technology companies, technical groups

[130] Lata Jha. "OTT platforms in a fix over offensive int'l content." Mint, May 27, 2023. https://www.livemint.com/industry/media/afwaahon-ka-safar-sunny-deol-reacts-on-drunk-viral-video-11701855316424.html; See also: Gerry Shih and Anant Gupta, "Facing pressure in India, Netflix and Amazon back down on daring films." The Washington Post, November 20, 2023. https://www.washingtonpost.com/world/2023/11/20/india-netflix-amazon-movies-self-censorship/; See also: Apar Gupta and Anushka Jain, "Tandav is a Case Study for OTT censorship under the IT Rules, 2021 #LetUsChill." Internet Freedom Foundation, March 27, 2021. https://internetfreedom.in/tandav-case-study/.

[131] Tejasi Panjiar and Prateek Waghre. "Dear MIB, Kill the Bill and #LetUsChill: Our Comments on the Broadcasting Bill, 2023." Internet Freedom Foundation, December 7, 2023. Accessed May 31, 2024.https://internetfreedom.in/comments-on-the-broadcasting-bill-2023/; See Also: Gerry Shih and Anant Gupta. "Facing Pressure in India, Netflix and Amazon Back down on Daring Films." Washington Post, November 21, 2023. Accessed May 30, 2024. https://www.washingtonpost.com/world/2023/11/20/india-netflix-amazon-movies-self-censorship/; See also: Aditya Kalra and Munsif Vengattil. "Worried about Obscenity, India Asks OTT Platforms for Content Checks." Business Standard, July 14, 2023. Accessed May 30, 2024. https://www.business-standard.com/industry/news/worried-about-obscenity-india-asks-ott-platforms-for-content-checks-123071400415_1.html; See also: Lata Jha. "OTTs Tread Cautiously, Cancel Shows | Mint." LiveMint, March 8, 2021. Accessed May 29, 2024.https://www.livemint.com/industry/media/otts-tread-on-cautious-ground-axe-shows/amp-11615188592226.html.

and members of the press.[132,133] UN Special Rapporteurs have called these Rules incompatible with "*international law and standards related to the right to privacy and to freedom of opinion and expression*" and sought their withdrawal.[134] IFF has published detailed analyses on rights issues arising from the Rules.[135]

In brief, the Rules empower MIB to exercise overbroad and arbitrary censorship of content. In recent history, MIB has invoked Rules 16 and 69A of the IT Rules and Act respectively to issue directions to intermediaries to block the BBC documentary 'India: The Modi Question', the blocking order for which was neither published nor furnished under the RTI Act, 2005. Individuals who shared links to the BBC documentary had their tweets blocked. More recently, independent magazine The Caravan was asked to similarly take down its article pertaining to killings by the military stationed in Jammu & Kashmir.[136] Both takedowns follow a pattern of censoring content that critically examines or questions the use of power by the incumbent government and gravely injure India's democratic ethos. The secrecy and opacity surrounding the blocking order further make it difficult to ascertain the reasons and what component of the content triggers Rule 16 or other invoked provisions and gives MIB free reign to arbitrarily apply them to critical content.

---

[132] Daphne Keller. "Filtering out Free Speech: The Shreya Singhal Case and the Supreme Court." Indian Express, February 20, 2020. Accessed May 28, 2024. https://indianexpress.com/article/opinion/columns/filtering-out-free-speech-shreya-singhal-case-supreme-court-6220277/. See Also: "Shreya Singhal Case Was One of the Defining Rulings of Modern Internet Law." The Indian Express, January 17, 2020. Accessed May 31, 2024. https://indianexpress.com/article/opinion/columns/filtering-out-free-speech-shreya-singhal-case-supreme-court-6220277/. See also: "Letter to MEITY on withdrawal of IT Rules, 2021". Internet Freedom Foundation, March 23, 2021. https://drive.google.com/file/d/1elhs46khdMd2lTWTE4ReFCIi2s8IYuAU/view See also: "'New IT Rules against Fundamental Principle of News': Digipub Writes to Prakash Javadekar." The Wire, June 3, 2024. Accessed May 31, 2024. https://thewire.in/media/digipub-prakash-javadekar-it-rules-digital-media?ref=static.internetfreedom.in. See also: "What Is Traceability and Why Does WhatsApp Oppose It? | WhatsApp Help Center." Faq.whatsapp.com, June 3, 2024. Accessed May 30, 2024. https://faq.whatsapp.com/general/security-and-privacy/what-is-traceability-and-why-does-whatsapp-oppose-it. See also: Neeti Biyani and Amrita Choudhury. "Internet Impact Brief: 2021 Indian Intermediary Guidelines and the Internet Experience in India." Internet Society, November 8, 2021. Accessed May 31, 2024. https://www.internetsociety.org/resources/2021/internet-impact-brief-2021-indian-intermediary-guidelines-and-the-internet-experience-in-india/; See also: N. Ram (@nramind). February 27, 2021. https://twitter.com/nramind/status/1365542902164639748.

[133] "Statements Issued." Editors Guild of India, June 29, 2018. https://editorsguild.in/statements-issued/?ref=static.internetfreedom.in.

[134] Office of the United Nations High Commissioner for Human Rights. "Communication concerning India dated 19 May 2021." OHCHR, May 19, 2021. https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile.

[135] Krishnesh Bapat, Anushka Jain, Apar Gupta, and Tanmay Singh. "Deep Dive: How the Intermediaries Rules Are Anti-Democratic and Unconstitutional." Internet Freedom Foundation, February 27, 2021. Accessed May 29, 2024. https://internetfreedom.in/intermediaries-rules-2021/; See also: Anushka Jain, Devdutta Mukhopadhyay, Tanmay Singh, Krishnesh Bapat, and Apar Gupta. "Latest Draft Intermediary Rules: Fixing Big Tech, by Breaking Our Digital Rights?" Internet Freedom Foundation. February 25, 2021. Accessed May 31, 2024. https://internetfreedom.in/latest-draft-intermediary-rules-fixing-big-tech-by-breaking-our-digital-rights/; See also: "Letter to MEITY on withdrawal of IT Rules, 2021". Internet Freedom Foundation, March 23, 2021. https://drive.google.com/file/d/1elhs46khdMd2lTWTE4ReFCIi2s8IYuAU/view. See also: Rohin Garg. "Constitutional Questions against Unconstitutional Rules." Internet Freedom Foundation, March 11, 2021. Accessed May 29, 2024. https://static.internetfreedom.in/constitutional-questions-against-unconstitutional-rules/.

[136] Internet Freedom Foundation. "Statement: In Response to a Takedown Order by MIB, the Caravan Has Taken down Its Article Pertaining to Killings by the Army Stationed in Jammu & Kashmir." Internet Freedom Foundation, February 14, 2024. Accessed May 29, 2024. https://internetfreedom.in/in-response-to-a-takedown-order-by-mib-the-caravan-has-taken-down-its-article-pertaining-to-killings-by-the-army-stationed-in-jammu-kashmir/.

Multiple court orders that record the legal deficiencies and constitutional injuries caused by the IT Rules, 2021.[137] IT Rules, 2021 cause injury to the constitutional and democratic rights of Indian internet users. They are contrary to the mandate laid down in *Shreya Singhal* and warrant a complete recall.

IT Amendment Rules, 2022

The IT Amendment Rules, 2022 introduced changes in Part I and II of the IT Rules, 2021, that further raised some alarms for platform and content governance in India.[138] The Rules introduces vague, arbitrary, and undefined phrasing under sub-clauses (i) to (ix) of the amended Rule 3(1)(b) such as "*knowingly and intentionally communicates any misinformation or information*". Misinformation been neither been defined, nor has criteria for determining intent been specified. The Rules seek to establish, with the ostensible aim of providing users additional avenues for grievance redressal apart from Courts, Grievance Appellate Committee(s) ("**GAC**") i.e. an executive-constituted committee, that will make the union government the arbiter of permissible speech on the internet. GACs will adjudicate any appeal raised by aggrieved persons against decisions of intermediary-level grievance officers to remove or not remove content. It may also incentivise social media platforms and intermediaries to suppress any speech unpalatable to the government, as IFF has deeply analysed in a public brief.[139] GACs do not have any legislative basis and empower the government to censor speech on vague grounds, which are also not stated under Section 69A of IT Act, 2000 or Article 19(2) of the Constitution.[140] Their operations have also been shrouded in secrecy—despite beginning operations on March 01, 2023, as of May 2024, no GAC reviews or orders have been released.[141],[142]

---

[137] IFF has provided legal representation to LiveLaw Media Pvt. Ltd. before the Kerala High Court which directed the union government to not take coercive action against the petitioner under IT Rules, 2021. IFF is also representing Mr. T.M. Krishna in proceedings before the Madras High Court where a Division Bench stayed Rules 9(1) and 9(3) while observing that the oversight mechanism in the Rules may "*rob the media of its independence*".
See also: Tanmay Singh. "Kerala HC Grants a Stay of the Operation of Part III of the Intermediaries Rules, 2021 to LiveLaw." Internet Freedom Foundation, March 10, 2021. Accessed May 28, 2024.
https://internetfreedom.in/kerala-hc-grants-a-stay-of-the-operation-of-part-iii-of-the-intermediaries-rules-2021-to-livelaw/.
See also: "Table summarizing challenges to IT Rules, 2021 pending before High Courts." Internet Freedom Foundation, 2022. Accessed May 29, 2024.
https://docs.google.com/document/d/1kmq-AlRO1XpPaThvesl5xQq2nVkZv6UdmaKFAJ8AMTk/edit?ref=static.internetfreedom.in.
See also: Krishnesh Bapat, Anandita Mishra, and Tanmay Singh. "May Threaten 'Independence of Media': Madras HC on IT Rules.". Internet Freedom Foundation, September 17, 2021. Accessed May 28, 2024.
https://internetfreedom.in/madras-high-court-affirms-the-pan-india-stay-on-rule-9-3-of-the-it-rules-and-provides-relief-on-part-ii/
.
See Also: Challenge to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. W.P.Nos.13055 and 12515 of 2021.

[138] Ministry of Electronics and Information Technology, Government of India. "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2022." Gazette of India, Part II-Section 3-Subsection (i), October 28, 2022. https://egazette.nic.in/WriteReadData/2022/239919.pdf.

[139] Tejasi Panjiar and Prateek Waghre. "A Public Brief on the IT Amendment Rules, 2022." Internet Freedom Foundation, November 11, 2022. Accessed May 28, 2024. https://internetfreedom.in/legislative-brief-2024-budget/.

[140] Several grounds mentioned in Rule 3(1)(b), such as "misinformation", remain undefined and thus are vague, impossible to implement consistently and prone to misuse. This may cause social media platforms to become pro-active arbiters of permissible speech which is already resulting in issues given existing lack of natural justice, transparency and accountability.

[141] Tejasi Panjiar and Prateek Waghre. "1 Month of the GAC Felt like a Lifetime! We Wrote to Them Seeking Answers." Internet Freedom Foundation, April 5, 2023. Accessed May 29, 2024. https://internetfreedom.in/we-wrote-to-the-gac-seeking-answers/.

[142] "Letter to Grievance Appellate Committee requesting to furnish details on their composition and functioning." Internet Freedom Foundation, April 1, 2023. Accessed May 28, 2024.
https://drive.google.com/file/d/1FxoZPLh8ffCjI3r7Ur74eJmCIDP87n2L/view.

IT Amendment Rules, 2023

IT Amendment Rules, 2023 legitimises the establishment of State-run fact check units (**"FCU"**) tasked with identifying 'fake or false or misleading' online content related to the government.[143] Taking action against content identified by such FCU is listed as a due diligence requirement for intermediaries. In an event where intermediaries fail to/decide against taking action on content identified as "fake" or "false" by the FCU, they will risk losing their safe harbour protections.[144]

To this extent, we believe that the IT Amendment Rules 2023, are ultra vires Section 79 of the IT Act, seeing that the revocation of safe harbour for intermediaries must conform to subject matters laid down in Article 19(2) as laid down in *Shreya Singhal*. Vague terms like 'fake or false or misleading' content are not grounds enumerated in Art. 19(2) or Section 69A of the IT Act, 2000, and can cement the chilling effect on the fundamental right to speech and expression, particularly on news publishers, journalists, activists, etc.[145] The constitutional validity of the IT Rules, 2023 was challenged in a batch of petitions before the Bombay High Court (some assisted by IFF), which delivered a split verdict, and referred to a third judge.[146,147] During the initial hearing, the union government undertook not to constitute the FCU until the judgment was pronounced. However, the union government withdrew this undertaking while the matter was being referred to the third judge. The Bombay High Court rejected the petitioners' interim relief application to halt the constitution of the FCU until the judegment.[148] Subsequently, the Supreme Court stayed the order denying interim relief of extending the union government's undertaking to not constitute the FCU until pendency of proeedings before Bombay High Court.

---

[143] Rule 3(1)(b)(v), IT Amendment Rules, 2023.

[144] "Draconian Rules: on the Impact of the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023," The Hindu, April 9, 2023. Accessed May 28,2024. https://www.thehindu.com/opinion/editorial/draconian-rules-the-hindu-editorial-on-the-impact-of-the-it-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2023/article66717811.ece.
See also: Jal Khambata. "Indian Newspaper Society Calls for Withdrawal of New I-T Rules." Free Press Journal, April 12, 2023. Accessed May 29, 2024. https://www.freepressjournal.in/india/indian-newspaper-society-calls-for-withdrawal-of-new-i-t-rules.
Manish Singh. "Facebook, Google and Twitter Voice Concern over India's Fact-Checking Rule." TechCrunch, April 17, 2023. Accessed May 30, 2024. https://techcrunch.com/2023/04/17/us-tech-giants-voice-concern-over-india-s-fact-checking-rule/?ref=static.internetfreedom.in.

[145] Tejasi Panjiar and Prateek Waghre. "Statement on the Notification of the IT Amendment Rules, 2023." Internet Freedom Foundation, April 6, 2023. Accessed May 30, 2024. https://internetfreedom.in/statement-on-the-notification-of-the-it-amendment-rules-2023/.

[146] Gayatri Malhotra and Tanmay Singh. "In Kunal Kamra's Petition in the Bombay High Court, the Government Undertakes Not to Constitute Its Fact Check Unit." Internet Freedom Foundation, April 27, 2023. Accessed May 28, 2024. https://internetfreedom.in/in-kunal-kamras-petition-in-the-bombay-high-court-the-government-undertakes-not-to-notify-its-fact-check-unit/.
See Also: Gayatri Malhotra and Tanmay Singh. "In a Petition Filed by the Association of Indian Magazines' Challenging the Fact Check Amendments to IT Rules, 2021, the Bombay High Court Directs the Government to File Its Reply." Internet Freedom Foundation, June 7, 2023. Accessed May 29, 2024. https://internetfreedom.in/it-rules-2023-aim-bombayhc.

[147] Radika Roy. "Bombay HC Delivers Split Verdict in Challenge to IT (Amendment) Rules 2023." Internet Freedom Foundation, January 31, 2024. https://internetfreedom.in/bombay-hc-delivers-split-verdict-in/.

[148] Editors Guild of India v. Union of India & Ors, Civil Appeal Nos 4509-4511 of 2024.

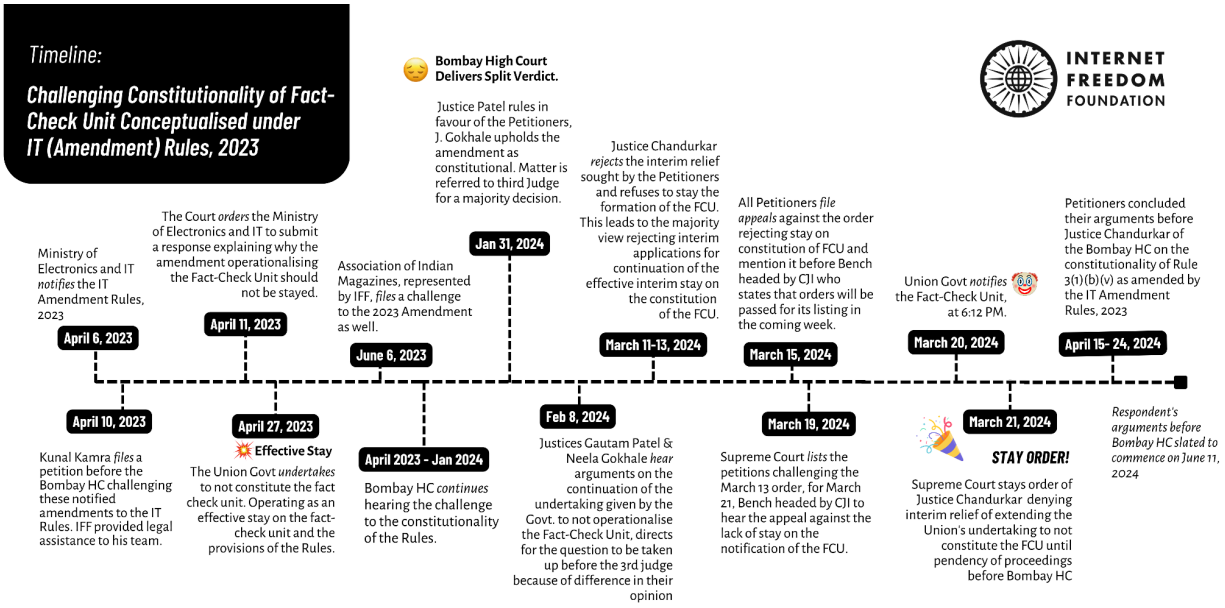

Image: Timeline as of 03 June, 2024 for the legal challenge and subsequent orders.

On March 20, 2024, MeitY notified the Press Information Bureau (**"PIB"**) as the FCU under the IT Amendment Rules, 2023.[149] Insufficient transparency and accessible information around the PIB FCU's composition and methodology for decision-making has previously raised questions about its capability and effectiveness.[150]

5. Threats to end-to-end encryption

In January 2020, India joined Japan in signing the Five-Eyes alliance stating that end-to-end encryption poses "*significant challenges to public safety*."[151] A year later, the IT Rules, 2021 were notified. The Alliance, along with India and Japan, stated their intent to build backdoors to end-to-end encrypted platforms for access to law enforcement agencies. This presents an undemocratic and unconstitutional framework for the regulation of online content.

Rule 4(2) requires significant social media intermediaries (**"SSMIs"**), which provide messaging services (such as Whatsapp), to enable identification of the "first originator" of a message on their platform if

[149] "Notifying Fact check unit under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021." Ministry of Electronics and Information Technology, March 20, 2024. https://content.internetfreedom.in/api/files/divco3ywedt9rpe/wddyt73l1imy0d5/253257_2_RLi51elIot.pdf?ref=static.internetfreedom.in

[150] Internet Freedom Foundation. "Statement: MeitY Has Notified the PIB Fact Check of MIB as the Fact-Checking Unit under the IT Amendment Rules, 2023." Internet Freedom Foundation, March 20, 2024. Accessed May 28, 2024. https://internetfreedom.in/statement-meity-has-notified-the-pib-fact-check-of-mib-as-the-fact-checking-unit/. See also: "Absurdity of an Interested Party Playing Judge': Newspapers Slam PIB Being Arbiter of 'Fake News." Newslaundry, January 20, 2023. Accessed May 29, 2024. https://www.newslaundry.com/2023/01/20/absurdity-of-an-interested-party-playing-judge-newspapers-slam-pib-being-arbiter-of-fake-news.

[151] U.S. Department of Justice. "International Statement: End-To-End Encryption and Public Safety." Justice.gov, October 11, 2020. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

required by a court of competent jurisdiction or a competent authority under Section 69A of the IT Act.[152] to enable identification of the "first originator" of a message. To implement this rule, entities will have to "fingerprint" each message and this may defeat end-to-end encryption (**"E2EE"**). As a consequence, the privacy of every user will be compromised to investigate crimes committed by a miniscule-minority. While the Rules clarify that traceability order may only be passed for serious offences, some categories are open-ended. For instance, "public order" grounds are relatively broad in operation and can give rise to many demands. They also clarify that in doing so, the SSMI shall not be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users. However, the IT Decryption Rules, 2009 contain powers to make demands for the message content.[153] Used together, the government may break any type of E2EE to gain knowledge of the sender of a message and also its contents. Also, this specific requirement will break existing protocols for the deployment of E2EE that has been built through rigorous cybersecurity testing over the years.

The Cyber Security Directions issued by Indian Computer Emergency Response Team ("**CERT-In Directions**") exacerbate concerns around collecting and storing of data beyond purpose or need through the requirements of "*mandatorily enabl(ing) logs of all… ICT systems and maintain(ing) them securely for a rolling period of 180 days* (Direction 4) and "*maintenance of data for 5 years or longer, as mandated by the law after any cancellation or withdrawal of registration*" for certain categories of data required for registration with data centres, Virtual Private Server Providers, cloud service providers and Virtual Private Networks service providers (Direction 5)."[154] Such requirements are against the principle of "storage limitation" related to the processing of data. The ambiguity around the time frame along with the lack of reasoning behind extending it could lead to serious privacy violations. Further, there are certain service providers such as Signal as well as certain VPNs such as Proton, which claim to not retain any logs due to their privacy respecting practices. These service providers may be forced to exit the Indian market as a result of these requirements. In fact, as a result of these Directions, several prominent VPN services such as ExpressVPN, NordVPN and Surfshark, have decided to stop doing business in India and ProtonVPN has classified India as a high-risk country.[155]

The definition of 'telecommunication' under the Telecommunications Act, 2023 leaves the scope of applicability wide enough for online communication services to be included within its ambit.[156] If internet services are included in the law's ambit, then the several alarming requirements related to surveillance, possession, suspension, authorisation, encryption etc. will be applied to those services as well, deepening the threats to our rights and freedoms. If the Telecommunications Act, 2023 becomes applicable to online

[152] Krishnesh Bapat, Anushka Jain, Apar Gupta, and Tanmay Singh. "Deep Dive: How the Intermediaries Rules Are Anti-Democratic and Unconstitutional." Internet Freedom Foundation, February 27, 2021. Accessed May 28, 2024. https://internetfreedom.in/intermediaries-rules-2021/.

[153] "The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009." Ministry of Communications and Information Technology. Accessed May 30, 2024. https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf.

[154] Tejasi Panjiar, Anushka Jain, and Prateek Waghre. "CERT-in Directions on Cybersecurity: An Explainer." Internet Freedom Foundation, May 5, 2022. Accessed May 30, 2024. https://internetfreedom.in/cert-in-guidelines-on-cybersecurity-an-explainer/.

[155] Krishnesh Bapat, "SnTHostings - a VPN, Seedbox and Root Server provider - urges MeitY to withdraw the unlawful CERT-In direction which will be effective from June 27, 2022." Internet Freedom Foundation, June 25, 2022. https://internetfreedom.in/snthostings-a-vpn-seedbox-and-root-server-provider-urges-meity-to-withdraw-the-unlawful-cert-in-direction-which-will-be-effective-on-june-27-2022/.

[156] Clause 2(p) read with 'telecommunication services' Clause 2(t), Telecommunications Act, 2023.

communication services, service providers such as WhatsApp, Signal etc., which adopt the privacy-protecting practice of E2EE, may also be required to intercept, detain, disclose, or suspend any message, wherein "message" is defined as "any sign, signal, writing, text, image, sound, video, data stream, intelligence or information sent through telecommunication."[157] Further, Section 20 includes the union government's power to temporarily possess, suspend, intercept, detain any telecommunication service, to intercept, detain, disclose, or suspend any message or class of messages, to direct suspension of any telecommunication service or class of telecommunication, or to notify encryption and data processing standards, cements the colonial powers of the union government, which upon misused and if extended to internet services, may become nothing less than draconian.[158]

6. Press harassment and intimidation

In 2021, 300 Indian phone numbers, including those belonging to Ministers, politicians, activists, researchers and journalists, were among the 50,000 reportedly targeted with an Israeli military-grade spyware, Pegasus.[159] Such spywares can only be deployed by hacking a phone that has been targeted by it. Compromising or hacking the phones of Indian citizens has no basis in Indian law. Statutory surveillance powers under the Telegraph Act, 1885 and Rules, and the IT Act, 2000 and Rules, do not permit the installation of spyware or hacking of mobile devices. In fact, such acts are criminalised under the IT Act, 2000.

The Pegasus incident was not dealt with the level of detail, care, or even gravity that it mandates. When use of the Pegasus spyware was reported in 2021, there was no investigation launched for two months.[160] Five journalists challenged the use of Pegasus on their phones before the Supreme Court, which culminated in the appointment of a committee of experts to investigate and enquire into the use of Pegasus on Indians—a case in which IFF provided legal assistance.[161] The Committee submitted its report before the Supreme Court in a sealed cover and its copy was not made available to the parties in the matter. Parts of the findings were read out, and it was concluded that malware was found in 5 out of 29 phones submitted, but this "*did not mean that it was Pegasus*." This directly contradicted global evidence but no opportunity was given to corroborate the claim through independent fact-checkers.[162]

Then on October 30, 2023, Apple, Inc. sent a threat notification to the mobile phones of opposition leaders, journalists, and researchers in India, which read "*state-sponsored attackers may be targeting your*

---

[157] Clause 2(g), Telecommunications Act, 2023.
[158] Clause [20(1)(a)], [20(2)(a)], [20(2)(b)], [19(f)], Telecommunications Act, 2023.
[159] "50,000 Phone Numbers Worldwide on List Linked to Spyware Pegasus." Deccan Herald, July 19, 2021. https://www.deccanherald.com/world/50000-phone-numbers-worldwide-on-list-linked-to-spyware-pegasus-1010275.html.
[160] Anushka Jain. "Pegasus Scandal: It's Been Two Months with No Investigation! #SaveOurPrivacy." Internet Freedom Foundation, September 13, 2021. Accessed May 29, 2024. https://internetfreedom.in/pegasus-2-months-on-still-no-investigation/.
[161] Krishnesh Bapat and Tanmay Singh. "Supreme Court of India Says: Investigate Pegasus!" Internet Freedom Foundation, October 27, 2021. Accessed May 30, 2024. https://internetfreedom.in/sc-appoints-a-committee-to-examine-the-use-of-pegasus-spyware-in-india/.
[162] Anandita Mishra and Tanmay Singh. "Pegasus Investigation Report to Remain in Sealed Cover despite Containing Evidence That 5 Phones Had Malware." Internet Freedom Foundation, August 26, 2022. Accessed May 30, 2024. https://internetfreedom.in/pegasus-investigation-report-to-remain-in-sealed-cover-even-though-it-contains-evidence-that-5-phones-had-malware/.

iPhone".[163] Apple claimed that this notification system detects state-sponsored attacks using the threat intelligence signals it receives, and is designed to inform and assist users who may be individually targeted owing to "*who they are or what they do*."[164] The Union Minister for Electronics and IT stated in a press conference the next day that though the notification was a "*vague and non-specific advisory*" and has gone out in 150 countries, a CERT-In investigation had been ordered to unravel it.[165] As with Pegasus, the Minister was seen downplaying the gravity of alleged targeted surveillance, and the investigation did not culminate into anything substantive.[166]

Targeted attacks and hacking of mobile phones are grave violations of privacy, as the device's cameras, microphones, and other functions can be manipulated and monitored without the user's knowledge or consent.[167] India's response to such a grave and direct crackdown on journalistic freedom has been lax at best. As seen with the Apple notification, such incidents are usually reported to CERT-In—but CERT-In's investigation is also limited in scope and jurisdiction to a technical and forensic evaluation of affected devices, and will not address the intent behind targeted state-sponsored attacks, the process of identifying targets, procurement and use of spyware by state actors, accountability, oversight, and legal safeguards.[168]

7. Sedition

In the past five years, there has been a notable misuse of Section 124-A of the Indian Penal Code, 1860 (**"IPC"**), with law enforcement agencies frequently invoking this charge in a manner that appears to lack substantial legal basis, raising concerns about arbitrary application of law and threats to free speech.[169] Insights from Article 14's empirical sedition database "A Decade of Darkness," support this claim with evidence, thereby indicating disregard for 'safeguards' set out by numerous judicial rulings by High Courts and the Supreme Court.[170,171] It also shows that 519 sedition cases were filed between 2014 and 2021, and a wide range of expressions were classified as seditious, including the mere holding of posters,

---

[163]Abhinav Anand. "Apple alert: All you need to know about threat notifications on iPhone." Financial Express, November 6, 2023. Accessed May 28, 2024. https://www.financialexpress.com/life/technology-apple-alert-all-you-need-to-know-about-threat-notifications-on-iphone-3298152/.

[164] "About Apple Threat Notifications and Protecting against Mercenary Spyware - Apple Support (IN)." n.d. Apple Support. https://support.apple.com/en-in/102174.

[165] "Opposition hacking claims: Apple advisory vague, issued in 150 nations, I-T Minister Ashwini Vaishnaw says." Times of India, October 31, 2023. Accessed May 28, 2024. http://timesofindia.indiatimes.com/articleshow/104851001.cms.

[166] "Cert-In investigation into Apple's state-sponsored threat notifications nears conclusion." The Economics Times, November 23, 2023. Accessed May 28, 2024. https://economictimes.indiatimes.com/tech/technology/cert-in-investigation-into-apples-state-sponsored-threat-notifications-nears-conclusion/articleshow/105453902.cms

[167] Anushka Jain. "The Arsenal Reports: Bhima Koregaon Arrests." Internet Freedom Foundation, August 21, 2021. Accessed May 30, 2024. https://internetfreedom.in/the-arsenal-reports-bhima-koregaon-arrests/.
See also: Ria Singh Sawhney and Raman Singh Chima. "In India, malware plants false 'evidence' of crime on activist's laptop." Access Now, May 19, 2021. Accessed May 30, 2024. https://www.accessnow.org/india-malware/.

[168]Apar Gupta. "Apar Gupta writes: Why government's defence on Apple spyware advisory is weak – and in bad faith", The Indian Express, November 2, 2023. https://indianexpress.com/article/opinion/columns/apar-gupta-writes-why-governments-defence-on-apple-spyware-advisory-is-weak-and-in-bad-faith-9009581/.

[169] "Sedition in India: Colonial Legacy, Misuse and Effect on Free Speech." Economic and Political Weekly, June, 7–8. Accessed May 30, 2024. https://www.epw.in/engage/article/sedition-india-colonial-legacy-misuse-and-effect.

[170] Kedar Nath Singh v. State of Bihar, (1962) AIR 955.
See also: Balwant Singh And Anr v. State Of Punjab, 1995 AIR SCW 2803.

[171] "A Decade of Darkness." Article 14. Accessed May 31, 2024. https://sedition.article-14.com/.

social media posts, the raising of slogans, and private communications.[172] In over 60% of these cases, additional laws such as the Unlawful Activities (Prevention) Act, 1967, the IT Act, 2000, the Arms Act, 1969, and the Criminal Law Amendment Act were appended to the FIRs. The database highlights rampant misuse of Section 124-A of the IPC, with some glaring and notable documented instances including:

- Social media users have faced 106 sedition charges for content deemed "anti-national" or in "support of Pakistan".
- During the farmers' protests, eight cases were filed against protestors; Protests against CAA/NRC resulted in 27 sedition cases.
- Journalists have faced 21 sedition cases, primarily since 2018, for reporting on farm laws, COVID-19, the Hathras gang rape, citizenship issues, and government criticism.
- 12 cases were filed against individuals for celebrating Pakistan's cricket victories over India, and another 12 during the COVID-19 pandemic for raising concerns over ventilators, food distribution, and migrant labour issues.

On May 11, 2022, the Supreme Court, after hearing a batch of petitions that challenged the constitutional validity of Section 124-A, issued a historic order, suspending all pending trials, appeals, and proceedings under the Section until the sedition law is re-examined.[173] Despite the Supreme Court's stay on the operation of the sedition law, state governments reportedly continued to file FIRs against individuals, charging them with sedition or threatening to impose sedition charges.[174] Subsequently, in June 2023, the 22nd Law Commission of India, in its 279th Report titled 'Usage of the Law of Sedition', recommended retaining the sedition provision, amongst other recommendations.[175] In September 2023, a three-judge bench of the Supreme Court referred the petitions challenging the constitutionality of the sedition law to a constitutional bench of at least five judges.[176] The Supreme Court has yet to constitute the Constitutional Bench.

---

[172] Kunal Purohit. "Our New Database Reveals Rise in Sedition Cases in the Modi Era." Article 14, February 2, 2021. Accessed May 30. https://www.article-14.com/post/our-new-database-reveals-rise-in-sedition-cases-in-the-modi-era.

[173] Krishnesh Bapat and Anandita Mishra. "In a Petition Filed by the Journalist union of Assam, Supreme Court Directs Governments to Not Use Section 124A." Internet Freedom Foundation, May 11, 2022. Accessed May 30, 2024. https://internetfreedom.in/jua-sc-sedition/.

[174] Vijaita Singh. "Manipur Violence | Sedition Case Against Meitei Politician After Assam Rifles Complaint." The Hindu, June 17, 2023. Accessed May 31, 2024. https://www.thehindu.com/news/national/meitei-politician-charged-with-sedition-for-defamatory-article-against-assam-rifles/article66977443.ece See Also: Vijaita Singh. "Assam Rifles Files Sedition Case against Imphal Civil Society Group." The Hindu, July 21, 2023. Accessed May 30, 2024. https://www.thehindu.com/news/national/assam-rifles-registers-case-against-influential-civil-society-group-in-imphal/article67106762.ece
Ridhi. "Manipur Violence and Sedition | Lawyer Booked for Accompanying Fact-Finding Team; Supreme Court Protects against Arrest." SCC Times, July 11, 2023. Accessed May 30, 2024.https://www.scconline.com/blog/post/2023/07/11/manipur-violence-supreme-court-protects-lawyer-against-arrest-sedition/
Debanish Achom. "Sedition Not Ruled out for Spreading Fake News, Misinformation on Manipur." NDTV.com, May 29, 2023. Accessed May 31, 2024. https://www.ndtv.com/india-news/sedition-not-ruled-out-for-spreading-fake-news-misinformation-on-manipur-4077017.

[175] Advay Vora. "Law Commission Recommends Stricter Sedition Law." Supreme Court Observer, June 3, 2023. Accessed May 29, 2024. https://www.scobserver.in/journal/law-commission-recommends-stricter-sedition-laws/.

[176] Radhika Roy and Tanmay Singh. "Supreme Court Refers Challenge to Constitutionality of Sedition Law to a Larger Bench of at Least 5 Judges." Internet Freedom Foundation, September 13, 2023. Accessed May 30, 2024. https://internetfreedom.in/sc-sedition-update-larger-bench/.

Annexure I

Aadhaar-related data breaches

In October 2023, a database claiming to contain sensitive personal details of 81.5 Crore Indian citizens, including their Aadhaar number, passport number, and other personal details, was found listed for sale on a dark web platform named 'BreachForums'.[177] Cybersecurity analysts reportedly found one of the leaked samples to contain 1,00,000 records of personally identifiable information, which included Aadhaar and passport numbers.[178] On November 01, 2023, the threat actor informed journalists that the database is "old" which they had bought from a now defunct dark web forum last year.[179] This is reported to be India's largest data breach yet. But it is not the first instance of a breach or leak of Aadhaar data.

1. In January 2018, The Tribune revealed that anyone could purchase the Aadhaar details of 1 billion registered citizens in "Rs 500 and 10 minutes" from anonymous sellers over WhatsApp.[180] The details included sensitive personal information such as names, bank details, addresses, and contacts. The same investigation revealed that over 1 Lakh ex-employees of MeitY continue to have free unauthorised access to the UIDAI system and the Aadhar database, further jeopardising its security.
2. In March 2018, ZDNet reported another data leak, this time through the systems of the state-run utility company Indane.[181] For weeks, the Indane website allowed anyone to download private information on all Aadhaar holders, exposing their names, their unique 12-digit identity numbers, a "consumer number" generated by Indane, and information about services they are connected to, such as their bank details. Indane had unlimited access to the Aadhaar database to verify user accounts, and an unprotected API endpoint through their system allowed anyone to make unauthorised queries on potentially all Aadhaar holders.
3. In May 2018, the Andhra Pradesh government accidently published over 1.3 Lakh Aadhaar numbers online, along with demographic and bank details.[182] The details were retracted after reports in the local media.
4. In September 2018, UIDAI's response to an RTI Application revealed that about 210 government

---

[177] Sarvesh Mathi. "Data Breach: Aadhaar And Passport Details Of 815 Million Indians Listed For Sale", Medianama, October 31, 2023. Accessed May 31, 2024. https://www.medianama.com/2023/10/223-aadhaar-815-million-indian-data-breach/.

[178] "Aadhaar data leak | Personal data of 81.5 crore Indians on sale on dark web: report", Economics Times Tech, October 31, 2023. Accessed May 31, 2024. https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms.

[179] Aihik Sur. "Just trying to recover my investment, says dark web threat actor selling 815 million Indians' database", MoneyControl, November 01, 2023. Accessed May 31, 2024. https://www.moneycontrol.com/news/business/just-trying-to-recover-my-investment-says-dark-web-threat-actor-selling-815-million-indians-database-11632341.html.

[180] "Rs 500, 10 minutes, and you have access to billion Aadhaar details", The Tribune India, January 03, 2018. Accessed May 31, 2024. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

[181] Zack Whittaker. "A new data leak hits Aadhaar, India's national ID database", ZDNet, March 23, 2018. Accessed May 31, 2024. https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/.

[182] Upmanyu Trivedi. "Aadhaar: World's largest ID database exposed by India government errors", The Economic Times, May 15, 2018. Accessed May 31, 2024. https://economictimes.indiatimes.com/news/economy/policy/worlds-largest-id-database-exposed-by-india-government-errors/articleshow/64169884.cms.

websites had so far made the Aadhaar details of Indian citizens public online.[183] It said the data was duly removed from the websites, but does not mention the time frame of the leak of the data. Reportedly, a simple google search could reveal thousands of databases comprising Aadhaar numbers, names, names of parents, PAN numbers, mobile numbers, religion, marks, the status of rejection of applications, bank account numbers, IFSC codes and other information.[184]

5. Further, in the first half of 2018 alone, a total of 1.2 Billion Aadhaar records were reportedly compromised, making it the second largest data breach of the year, globally.[185] These findings by the Breach Level Index, a database of public data breaches run by digital security platform 'Gemalto', were subsequently withdrawn for lack of evidence.[186]
6. In February 2019, a state web portal used to mark attendance of government employees in Jharkhand was left exposed and accessible without a password, showing Aadhaar data as far back as 2014, which allowed anyone access to names, job titles, and contact of over 1.6 Lakh employees.[187] The portal could be easily discovered through the Jharkhand government's website, and was indexed by Google, which reportedly "*cached copies of not only the site itself, but also its attendance record pages that still contain Aadhaar numbers in each worker's photo*."[188]
7. The Sevamitra app designed by IT Grids Pvt. Ltd. for the Telugu Desam Party collected polling booth-level voter data in Telangana and Andhra Pradesh. Through this, in April 2019, the company was able to illegally access the Aadhaar data of 7.8 Crore Indians, and was booked by the Telangana police for data theft.[189] UIDAI deferred the alleged lack of security measures to SRDHs.
8. In 2021, the Tamil Nadu Civil Supplies and Consumer Protection Department, which held personal information and ration cards of 6.76 Crore residents at the time, suffered a breach that led to the Aadhaar details of about 50 Lakh people being put for sale on a hacker forum.[190] Details included addresses, mobile numbers, Aadhaar numbers, and family information.
9. In June 2022, a section of the Indian government's Pradhan Mantri Kisan Samman Nidhi website exposed Aadhaar-related information of 11 Crore farmers enrolled under the scheme.[191]

---

[183] "Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected", Firstpost, September 25, 2018. Accessed May 31, 2024. https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html.

[184] Ibid.

[185] "1.2 billion Aadhaar records compromised in first half of 2018: Gemalto report", MoneyControl, October 23, 2018. Accessed May 31, 2024. https://www.moneycontrol.com/news/india/1-2-billion-aadhaar-records-were-compromised-in-the-first-half-of-2018-gemalto-3053001.html.

[186] "Gemalto withdraws report that claimed data breach at Aadhaar", MoneyControl, October 23, 2018. Accessed May 31, 2024. https://www.moneycontrol.com/news/india/gemalto-withdraws-report-that-claimed-data-breach-at-aadhaar-3076281.html.

[187] Zack Whittaker. "Indian state government leaks thousands of Aadhaar numbers", Tech Crunch, February 01, 2019. Accessed May 31, 2024. https://techcrunch.com/2019/01/31/aadhaar-data-leak/.

[188] Ibid.

[189] "AP data theft: SIT claims IT Grids also has Telangana data in app", Livemint, March 07, 2019. Accessed May 31, 2024. https://www.livemint.com/news/india/ap-data-theft-sit-claims-it-grids-also-has-telangana-data-in-app-15519734296l8.html. See: "IT Grids Aadhaar data theft case may be the biggest ever in India: experts", Times of India, April 15, 2019. Accessed May 31, 2024. http://timesofindia.indiatimes.com/articleshow/68880147.cms.

[190] Aroon Deep. "Tamil Nadu PDS System Breached, 50 Lakh People's Aadhaar Details Leaked: Report", June 30, 2021. Accessed May 31, 2024. https://www.medianama.com/2021/06/223-tamil-nadu-pds-system-breach/.

[191] "New Aadhaar data leak exposes 11 crore Indian farmers' sensitive info", Zee News, June 14, 2022. Accessed May 31, 2024. https://zeenews.india.com/personal-finance/aadhaar-data-breach-over-110-crore-indian-farmers-aadhaar-card-data-compromised-2473666.html.

Annexure II

Data breaches in public databases at the Union and state level

1. In early October 2023, the National Logistics Portal exposed sensitive credentials and secret encryption keys through publicly accessible JS files on its website. Furthermore, numerous Amazon Web Services S3 buckets containing personal data such as worker information, marine crew details, invoices, and internal documents were found to be openly accessible to the public.
2. The state-owned telecom operator Bharat Sanchar Nigam Ltd reportedly suffered a significant data breach, exposing sensitive personal data such as email addresses, billing details, contact numbers, mobile outage records, network details, completed orders, and customer information.[192] .
3. The System for Pension Administration Raksha portal, a dedicated government pension portal for defence personnel, allegedly suffered a data breach which resulted in the leak of sensitive information such as usernames, passwords, pension numbers, and more of thousands of defence personnel.[193] In a worrying development, access credentials to this sensitive information emerged on Telegram, posing a risk of potential misuse and manipulation of vital pension-related processes.
4. Reportedly, Madhya Pradesh e-Nagarpalika portal suffered a cyber attack which corrupted the entire data of 413 cities and towns covered under the portal.[194] The portal oversees welfare service delivery mechanisms such as birth and death as well as marriage certificates, payment of property, water and sanitation taxes, etc.
5. On December 22, 2021, a cyber-security researcher identified a vulnerability in the Andhra Pradesh Directorate of Government Examination website which put the sensitive personal information of minors at risk of misuse.[195] The website suffered from a vulnerability that enabled any person to access and also edit the sensitive personal data of minors including their caste location, religious affiliation, and their disability status.

[192] Dia Rekhi, "BSNL suffers data breach; sensitive info of users up for sale on dark web." The Economic Times, December 22, 2023. https://telecom.economictimes.indiatimes.com/news/industry/bsnl-suffers-data-breach-sensitive-info-of-users-up-for-sale-on-dark-web/106197459; See also: IFF's letter on the BSNL data breach numbered IFF/2023/060, December 27, 2023. https://drive.google.com/file/d/1EkTNIDjS4WwVK6edRVBO22CZsp-tm4dd/view.

[193] Samiksha Jain, "TCE Exclusive: Massive Data Leak at India's SPARSH Pension Portal Puts Defense Personnel at Risk." The Cyber Express, 8 January 2024. https://thecyberexpress.com/sparsh-portal-data-leak-exposes-sensitive-info/.
See also: IFF's letter on the SPARSH data breach numbered IFF/2024/007, January 12, 2024. https://drive.google.com/file/d/1saYziL2X6a9encIgW7t2Rp3jh4Gxi1sg/view.

[194] Press Trust of India, "MP's e-Nagarpalika portal covering 413 urban areas suffers cyber attack, data corrupted." Economic Times Government. December 24, 2023. https://government.economictimes.indiatimes.com/news/secure-india/mps-e-nagarpalika-portal-covering-413-urban-areas-suffers-cyber-attack-data-corrupted/106244138.

[195] Tejasi Panjiar, "Student data exposed on Andhra Pradesh Government Examination website!." Internet Freedom Foundation, February 04, 2022. https://internetfreedom.in/ap-gov-students-data-leak/

Internet Freedom Foundation I-1718, Third Floor,
Chittaranjan Park, New Delhi 110019

policy@internetfreedom.in
internetfreedom.in