Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**575**
Land:	Indien
Kilde:	Freedom House
Titel:	Freedom on the Net 2024 – India
Udgivet:	16. oktober 2024
Optaget på baggrundsmaterialet:	7. november 2024

Freedom House

FREEDOM ON THE NET 2024

India

PARTLY FREE

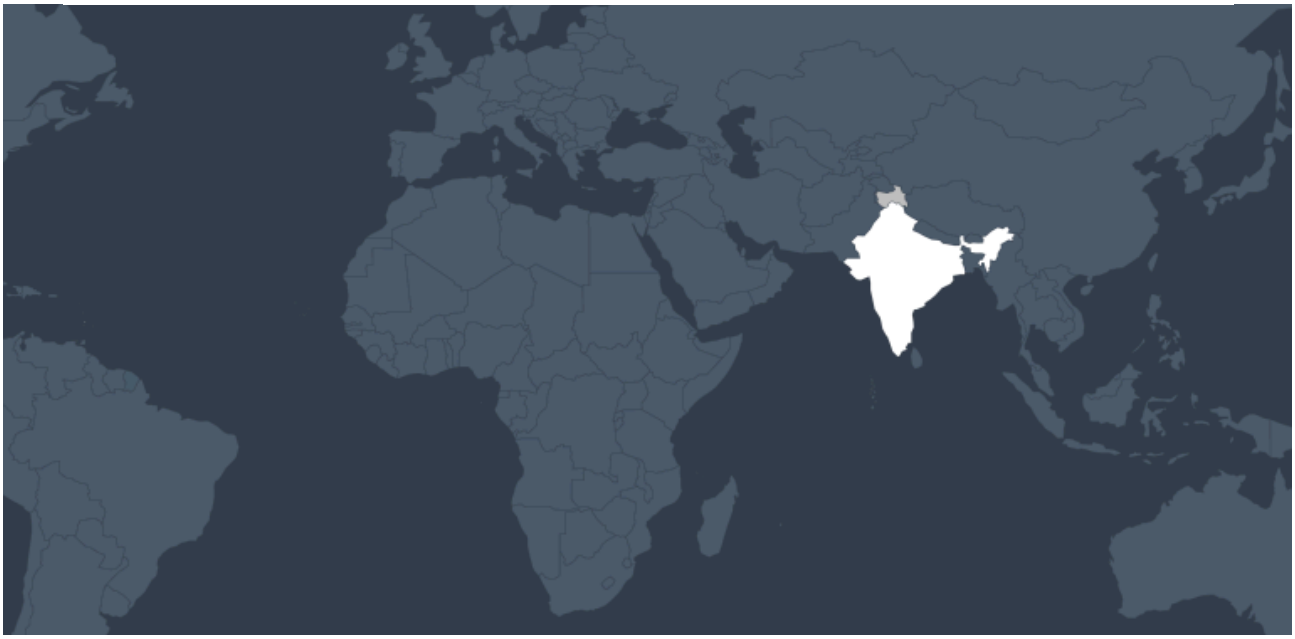
50 /100

A. Obstacles to Access	14 /25
B. Limits on Content	19 /35
C. Violations of User Rights	17 /40

LAST YEAR'S SCORE & STATUS

50 /100 **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.



Key Developments, June 1, 2023 – May 31, 2024

Internet freedom in India remained under strain during the coverage period. The government continues to impose internet shutdowns and censor online content, and Indian internet users risk arrest for posts critical of the government. Misinformation and disinformation are frequently shared online, and journalists, activists, and members of marginalized groups are often targeted by hate speech and harassment online.

- The new Telecommunications Act, passed in December 2023, overhauls India's telecommunications regulatory framework, affording the government broad powers to restrict online communications and intercept communications (see A3, A4, C4, and C5).
- During the 2024 election period, authorities ordered the blocking and removal of online content on political issues, including criticism of the government and independent reporting (see B1 and B2).
- Online information was manipulated by political parties and campaigns, particularly the ruling Bharatiya Janata Party (BJP), and new disclosures reported that the Indian military had manipulated sought to influence public perceptions on Jammu and Kashmir through influence operations (see B5).
- In December 2023, the legislature passed the Bharatiya Nyaya Sanhita (BNS), a criminal code meant to replace the penal code; though the BNS removes the colonial-era sedition clause, it contains several provisions that criminalize online expression on political and social issues (see C2).
- People were frequently investigated or arrested for their online activity, including the founder and editor in chief of news site NewsClick, who was held in pretrial detention for over six months on charges relating to the outlet's editorial stances and on allegations that it received funding from China (see C3).

Political Overview

While India is a multiparty democracy, the government led by Prime Minister Narendra Modi and the BJP has presided over discriminatory policies and a rise in persecution affecting Muslims. The constitution guarantees civil liberties including freedom of expression and freedom of religion, but harassment of journalists, civil society organizations (CSOs), and other government critics has increased significantly under Modi. The BJP has increasingly used government institutions to target political opponents. Muslims, scheduled castes (Dalits), and scheduled tribes (Adivasis) remain economically and socially marginalized. The April–June 2024 parliamentary elections saw Prime Minister Modi secure a third term, heading a coalition government for the first time in his tenure.

Note: Indian Union Territory of Jammu and Kashmir is not covered in this report. Certain territories that are assessed separately in Freedom House's Freedom in the World *report are excluded from the relevant country reports in* Freedom on the Net*, as conditions in such territories differ significantly from those in the rest of the country.*

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**4**/6

Score Change: The score improved from 3 to 4 because median mobile internet speeds have improved in recent years.

While internet penetration among India's population of over 1.4 billion is relatively low, access to the internet continues to rise. The Telecom Regulatory Authority of India (TRAI) reported 954.4 million internet subscribers as of August 2024, an internet penetration rate of approximately 65.8 percent. **1** By contrast, the digital analytics company DataReportal's Digital 2024 analysis identified a national penetration rate of 52.4 percent as of February 2024. **2** The Department of Telecommunications (DoT) has reported that 608,353 of the more than 644,000 villages in India have wireless broadband coverage. **3** The yearly growth rate of internet subscription has declined in recent years, from 19 percent in 2019 to 2.5 percent in 2023. **4**

India's median connection speeds as of April 2023 were 100.65 megabits per second (Mbps) for mobile service and 62.07 Mbps for fixed-line broadband service. [5] Nearly 97 percent of subscribers accessed the internet through mobile devices as of December 2023, with only 33.9 million having wired internet connections, per TRAI data. [6]

Several public- and private-sector initiatives aim to improve internet access. The government has set up over 149,000 public Wi-Fi hotspots under the prime minister's Wi-Fi Access Network Interface (PM-WANI) scheme as of August 2023. [7] The finance minister announced in February 2022 that the government planned to launch 5G mobile network spectrum by 2023, and aims to connect all villages via fiber-optic cable by 2025 to enable affordable broadband. [8] As of May 2023, 400,000 5G sites have been rolled out across India, [9] and the DoT launched a multistakeholder collaboration to drive innovation in 6G technology in July 2023. [10]

Launched in 2011, the government's BharatNet project has aimed to provide broadband connectivity to all the 250,000 gram panchayats ("village councils," units of local self-governance at the village level) in India; [11] that project has faced several delays and challenges (see A2). [12] As of December 2023, the initiative connects over 210,000 gram panchayats. [13] RailTel, a public-sector undertaking under the Ministry of Railways, aims to provide free Wi-Fi access at railway stations, with 6,100 stations connected as of March 2022. [14]

The National Internet Exchange India (NIXI), a nonprofit organization set up to facilitate peering between internet service providers (ISPs) and improve internet services, announced plans in March 2022 to establish 16 additional internet exchanges to improve internet access. [15]

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

While mobile data plans in India are inexpensive, digital divides remain across geography, language, economic class, and gender. [16] According to a 2023 report from the UK-based company Cable, the average cost of one month of broadband

services in India is $10.11. [17] Access to inexpensive mobile data has served to bridge the digital gender divide by allowing more women to access the internet to participate in markets, join community discourse, and build networks. [18] The Indian government maintains its stance on net neutrality by barring differential pricing for data services. [19]

TRAI reported 556.1 million internet subscribers in urban areas and 398.4 million rural subscribers as of March 2024, representing 111.8 percent internet penetration in urban areas and 44.2 percent internet penetration rate in rural areas. [20] Several initiatives aim to narrow the urban-rural divide, [21] such as the PM-WANI (see A1). [22] The government's Digital India Programme, launched in 2014, [23] plans to extend fiber-optic cables to more rural areas, [24] establish internet-connected common service centers (CSCs), [25] and provide residents with e-literacy programs. [26]

Despite delays in implementation and uneven progress made among states, [27] the government-led BharatNet project has successfully connected over 80 percent of gram panchayats as of January 2024. [28] The comptroller and auditor general of India reportedly found in July 2021 that the maintenance of cable and other infrastructure under the BharatNet project was inadequate in places, resulting in poor service quality. [29] The deadline for completion of the BharatNet project has been extended to 2025; [30] some forecasts suggest that the project will not meet that target. [31] Some people in BharatNet-connected gram panchayats have reported that limited and unreliable internet access. [32]

A significant gender divide persists. [33] According to the 2019–21 National Family Health Survey, only 33 percent of adult women have access to the internet, as opposed to 57.1 percent of men. [34] The divide is particularly pronounced in rural areas, and rates of access also vary between states. [35] The 2023 *Annual Status of Education Report* found that boys between the ages of 14 and 18 are over twice as likely to own smartphones than girls, who also lag behind in device proficiency. [36]

With 22 official languages, language remains a barrier to access in India. As of February 2021, the .bharat domain was available in all official languages. [37] According to a December 2021 study by Meta, 91 percent of online interaction by women is conducted in English, indicating that access to social media is functionally limited to English-speaking women. [38]

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**2** / 6

India has been the global leader in the number of internet shutdowns imposed for the last five years, [39] and local authorities have restricted connectivity since at least 2010. [40] While the frequency, geographic distribution, and duration of internet shutdowns had been increasing, the number of internet shutdowns has reduced in recent years: The Internet Shutdown Tracker from the Software Freedom Law Center (SFLC) reported 132 internet shutdowns in 2020, 100 in 2021, 77 in 2022, 96 in 2023, and 42 in 2024 as of September. [41] Since the government does not track internet shutdowns across the country, they are monitored by CSOs using newspaper reports, right-to-information requests, and anecdotal evidence. Authorities typically justify shutdowns as cautionary measures to maintain law and order, [42] quell potential violence or communal tensions, [43] restrict protests, [44] prevent the spread of disinformation, or stop cheating in school exams. [45]

Authorities enforced an internet shutdown in the state of Manipur that lasted over 208 days in 2023, according to data compiled by Top10VPN. [46] Authorities first restricted internet access across Manipur in May 2023; members of the predominately Hindu Meitei and largely Christian Kuki communities had been involved in violent clashes after Kuki residents objected to a court order granting scheduled-tribe status to the majority Meitei. The Manipur government conditionally restored some fixed-line connectivity in July 2023, and access more broadly in September 2023. [47] Shutdowns continued intermittently in some districts throughout the coverage period until February 2024. [48] These internet outages impeded the documentation of and response to acts of violence, including sexual violence, perpetrated during the conflict. [49] Manipur authorities imposed connectivity restrictions during subsequent escalations of the conflict, including in September 2024, after the coverage period. [50]

Authorities enforced shutdowns during protests. In February 2024, the Union government and government of the state of Haryana imposed a two-day shutdown in several parts of Haryana and Punjab amid farmers' protests. [51]

Authorities in the state of Maharashtra suspended internet services for half a day in Beed District as protesters there marched to demand greater inclusion for the Maratha castes in the Other Backward Classes (OBC) category. The shutdowns were imposed following violence and targeting of the houses and offices of political representatives in Beed. [52]

In the Jammu and Kashmir region, which is excluded from this report's scoring (see Overview), the state administration ordered the longest internet shutdown in India's history between August 2019 and January 2020—a total of 213 days—in the wake of the central government's abrogation of Article 370 of the Indian constitution, which provided special status to the state. [53] However, internet shutdowns in the region notably decreased from 43 in 2022 to 10 in 2023. [54]

Most of India's internet infrastructure is privately owned by service providers, and the government relies on legislative and statutory mechanisms to order shutdowns. Orders to restrict connectivity have been justified under Section 144 of the 1973 code of criminal procedure (CrPC), which permitted state actions to maintain law and order. [55] The Bharatiya Nagarik Suraksha Sanhita (BNSS), which was passed to replace the CrPC in December 2023 and took effect in July 2024, after the coverage period, contains a similar provision. Though courts had previously upheld the use of this law to order shutdowns and had refused legal challenges on this basis, observations by the Supreme Court in 2020 have resulted in some experts suggesting that Section 144 should not have been utilized to authorize shutdowns. [56]

Authorities in India also use Section 5(2) of the Telegraph Act, 1885, to order internet shutdowns. Section 5(2) provides government authorities with the power to stop the transmission of messages or classes of messages in the event of a public emergency or for public safety. [57] The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, under Section 7 of the Telegraph Act, [58] authorize only national- or state-level officials of a certain rank to order temporary suspensions in times of public emergency or threats to public safety, [59] and mandate that each order must be justified and be forwarded to a review committee for assessment. [60] The Supreme Court directed in January 2024 that the review committee established for overseeing internet-shutdown directions issued by Jammu and Kashmir authorities must publish its orders to ensure proper checks and balances. [61] However, several shutdown orders since

2017 were issued under Section 144 of the CrPC by officials not designated under the Telegraph Act rules, [62] sparking concerns from CSOs that procedural safeguards and checks were not followed. [63] In November 2020, the government amended the rules to specify that a shutdown order could not be in effect for more than 15 days, but such orders could be renewed. [64] Civil society criticized a lack of consultation and public participation in crafting the amendment, and condemned the provision allowing authorities to continually renew the order. [65]

In December 2023, Parliament passed the Telecommunications Act, 2023, to update the country's telecommunications legal framework; [66] the law retains many of the powers granted to the government under the Telegraph Act and the Temporary Suspension of Telecommunications Service Rules. While suspension orders must be in writing, and must rely on clear reasons, the act offers no other limitations of safeguards. [67] As in the Telegraph Act, the new law grants officials the authority to temporarily halt, suspend, intercept, and detain transmissions and messages "in the interest of the sovereignty and integrity of India" and "public order," among other broad justifications. [68] The new law also grants authority to either the Union government or a state government to assume control of any telecommunication service or network during a public emergency or safety concern. [69] In August 2024, after the coverage period, the Ministry of Communications released draft rules to operationalize the Telecommunications Act, including rules on suspension of services. [70]

Courts have directly ruled on the legality of restrictions and in some cases ordered restored services. [71] In March 2022, during the previous coverage period, the Calcutta High Court stayed an internet shutdown order issued by the state of West Bengal to prevent cheating in school exams—only the second time an Indian court stayed such an order, according to the Internet Freedom Foundation (IFF). [72]

In response to the monthslong shutdown in Jammu and Kashmir, [73] the Supreme Court ruled in January 2021 that orders for connectivity restrictions must be publicly available and should be well reasoned, proportionate, temporary, and present the least restrictive alternative. [74] However, compliance with the ruling remains unclear. [75] In February 2022, the government stated in response to a query by a member of Parliament (MP) that records of internet shutdowns ordered by state governments are not maintained. [76] In September 2023, the

Jharkhand High Court ordered the state to publish all past internet shutdown orders. [77]

The government has ordered the blocking of hundreds of mobile apps since 2020, [78] primarily those owned by companies based in China, citing concerns related to national security, public order, and Indian sovereignty. [79] In December 2023, the Ministry of Electronics and Information Technology (MeitY) reported that it had blocked a total of 581 apps, which included 174 gambling apps and 87 loan-lending apps. [80]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**4**/6

Internet users have a range of choices for telecommunications connections. While fees to enter the market have served as an economic barrier for some providers, there are no significant obstacles to entry for service providers.

As of September 2024, there almost 1,200 operational ISPs in India, the vast majority of which are last-mile providers with small subscriber bases. [81] Per TRAI data from March 2024; the top three service provides—Reliance Jio (51.4 percent), Bharti Airtel (31 percent), and Vodafone Idea (15 percent) together control the preponderance of the wireless-internet market segment. In the wired-internet market segment, Reliance Jio controls 28 percent, followed by Bharti Airtel at 19.2 percent and the state-run Bharat Sanchar Nigam, Ltd. (BSNL) at 10.1 percent. [82]

Facebook invested in a 9.9 percent stake in Reliance Jio in April 2020, [83] while Google purchased a 7.7 percent stake in Jio Platforms, which owns Reliance Jio, in November 2020. [84] In January 2022, Google invested in a 1.3 percent stake in Bharti Airtel, among other agreements with the company. [85]

A 2014 universal license framework [86] reduced legal and regulatory obstacles by combining mobile phone and ISP licenses. Licensees pay a high one-time entry fee, a performance bank guarantee, [87] and annual license fees adjusted for revenue. [88]

The Telecommunications Act, passed in December 2023, establishes an "exclusive privilege" for the Indian government to provide telecommunication services in India. The law requires government authorization to provide telecommunications services, and establish, operate, maintain, or expand a telecommunications network. [89] The law has been criticized for not meaningfully defining "telecommunication services," creating ambiguity over (over-the-top) OTT content providers, online content hosts, and communication platforms such as Signal and WhatsApp. [90] Though officials publicly stated that such OTT services would not fall under the Telecommunications Act, the law remains ambiguous. [91] It is unclear whether service providers would be required to comply with the bill's onerous obligations for internet suspension, communications interception, and user identification to maintain their license (see A3, C4, and C5). The IFF and other CSOs raised concerns that the law failed to meaningfully reform telecommunications regulation and could subject service providers to onerous requirements, including on surveillance. [92]

In October 2019, a Supreme Court decision clarified that the percentage of revenues that license holders must pay the government is calculated on the basis of the entire revenue of the license holder, and not just revenue from telecommunications services. [93] In September 2020, the court passed an order giving telecommunications companies 10 years to pay their dues. [94] In October 2023, the Supreme Court ruled that service providers like Bharti Airtel and Vodafone Idea must treat the license fee paid to the DoT after July 1999 as capital expenditure, not revenue expenditure. [95] Consequently, Vodafone Idea converted its adjusted-gross-revenue dues into equity in January 2022, making the government that company's largest shareholder. In December 2023, Minister of State for Communications Devusinh Chauhan informed lawmakers that the government has no plans to run or take control of Vodafone Idea. [96]

Roughly 15 submarine cables connect India to the global internet, [97] most of which are consortium-owned. [98] There are at least 15 landing stations where the cables meet the mainland, spread across five cities, [99] with eight more landing stations expected to be ready by 2025. [100] Currently, Tata Communications owns five cable landing stations, Reliance Jio owns two, and Bharti Airtel owns three. [101] The state-run BSNL owns three landing stations, and Vodafone, Sify, and Global Cloud Exchange own one each. [102]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**2** / 4

The MeitY formulates policy relating to information technology, electronics, and the internet. [103] The DoT, under the Ministry of Communications, manages the overall development of the telecommunications sector, licenses service providers, and manages spectrum allocation. [104]

The TRAI regulates the telecommunications, broadcast, and cable television sectors. [105] The TRAI Act mandates transparency in the exercise of its operations, which includes monitoring licensing terms, compliance, and service quality. [106] Its reports are published online, usually preceded by a multistakeholder consultation. [107] A 2000 amendment to the TRAI Act established a three-member Telecommunications Dispute Settlement and Appellate Tribunal. [108]

There have been some reservations about TRAI's independence. [109] The central government makes appointment and salary decisions for its members. [110] Amendments to the TRAI Act enacted in 2014 allow former government officials to join the regulator two years after resigning from office, or earlier with government permission. [111] TRAI opinions, however, are generally perceived as free of undue influence, and the regulator engages in public consultations. [112] For example, TRAI sought stakeholder comments in December 2021 on creating a licensing framework to establish satellite gateways, which would help increase access to broadband services in India. [113]

The MeitY's Grievance Appellate Committees (GACs) became operational in March 2023, and will allow users to appeal decisions taken by social media platforms on content moderation (see B3). Three GACs established in January 2023 are comprised primarily of former military officials, police, and civil servants, [114] raising concerns about the committees' independence.

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	3/6

Political and social information is regularly blocked by court or government orders in India. Although these orders are not always publicly released, government data show an increasing number of requests.

In December 2023, the MeitY minister stated in Parliament that 7,502 accounts, websites, and URLs had been restricted on government orders in 2023 under Section 69A of the Information Technology (IT) Act, 2000. The government stated that it had banned a total of 36,800 URLs between 2018 and 2023, over 13,600 of which were on X. [115] Blocking orders are often substantiated for content allegedly seeking to stoke anti-India sentiment, or to harm public order, state security, or sovereignty and integrity. [116]

Authorities frequently block websites featuring social or political expression, including criticism of the government. For example, in August 2023, Indian authorities blocked access to the Jammu and Kashmir–based outlet Kashmir Walla across the country. [117]

Authorities sometimes restrict access to social media platforms. In May 2024, authorities in Bihar blocked over 20 social media platforms, including WhatsApp, for several days in Saran District, citing the need to limit the spread of a local conflict. [118]

Several reports have clarified the technology used to block websites in India. The SFLC reported in January 2023 that techniques used by ISPs to implement website blocking include domain name system (DNS) tampering; HTTP blocking; transmission control protocol/internet protocol (TCP/IP) blocking; transport layer security–server name indication (TLS-SNI) blocking; and Quick User Datagram Protocol Internet Connection (QUIC) network blocking. [119] The Open Observatory of Network Interference (OONI) and the Centre for Internet and Society previously reported that Bharti Airtel and Reliance Jio use SNI-based filtering to restrict access to websites on government orders. [120] In April 2018, Canadian internet watchdog Citizen Lab found that India was using internet-filtering technology from the Canada-based company Netsweeper. [121]

Service providers appear to restrict different sets of websites. For instance, security researchers identified over 5,000 websites blocked on Atria Convergence Technology's fixed-line broadband services and over 2,000 websites blocked on Bharti Airtel's networks, per a December 2021 report. [122]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**1** / 4

Government actors regularly order social media and other online platforms to remove content, including material protected under international human rights standards. The IT Rules, 2021, provide a regulatory framework for online publishers of news and current affairs and curated audiovisual content (see B3). They also give the state emergency powers to block content without a hearing, which have been invoked by the authorities at times. [123] Content restricted under Section 69A of the IT Act increased in 2023, with 7,502 blocked websites and accounts disclosed that year, compared to 6,935 blocked items being disclosed in 2022; the disclosures likely represent both website blocks and takedowns from content hosts (see B1). [124]

Government agencies issued content removal orders during the electoral period, including criticism of political candidates and the ruling BJP. In April 2024, X removed four posts, including one from the official Aam Aadmi Party (AAP) account and another from a senior BJP official, pursuant to an order from the Election Commission of India (ECI), which cited a clause of the model code of conduct. [125] That code governs the conduct of candidates and parties during elections, and does not empower the ECI to order online content removed barring criticism of the private life of public officials. [126] The AAP post criticized Prime Minister Modi over the electoral-bonds scheme, prompting concern about the ECI's removal order. [127]

In February 2024, the MeitY issued an emergency order at the request of the Ministry of Home Affairs (MHA), directing blocks targeting 177 social media accounts and links associated with farmers' protests, citing public order. [128] The

blocked accounts included those belonging to farmers participating in the protests, journalists from Punjab and Haryana, Dalit activists, and local CSOs. [129]

Other content removal orders are related to independent reporting and research. In February 2024, *Caravan* was directed by the Ministry of Information and Broadcasting (MIB) to take down an article it had published, under Section 69A of the IT Act. The article reported on the purported torture and deaths of villagers in Jammu and Kashmir, allegedly involving the army. [130] In April 2024, the MIB instructed YouTube to block the channels of two popular Hindi news outlets, Bolta Hindustan and National Dastak, citing Section 69A. [131] In January 2024, X withheld the account of Hindutva Watch, a research project documenting anti-Muslim violence and rhetoric, under Section 69A. [132]

Though data on content removal orders is not publicly available, research indicates that compliance is common. Analysis from news site Rest of World found that—according to public disclosures in the Lumen database—the social network then known as Twitter complied in full or in part with all 44 removal orders filed by the Indian government from the time that the platform was acquired by Elon Musk in late October 2022 to late April 2023. [133]

A 2008 IT Act amendment protected technology companies from legal liability for content posted to their platforms, with reasonable exceptions to prevent criminal acts or privacy violations. [134] In the 2015 *Shreya Singhal v. Union of India* ruling, the Supreme Court had reduced the scope of the 2011 intermediary guidelines, and companies were only to act on court and government takedown orders and not on user complaints. The court also clarified that unlawful content beyond the scope of Article 19(2) of the constitution—which sets forth certain restrictions on the right to the freedom of speech and expression—cannot be restricted. [135] In November 2023, then government minister Rajeev Chandrasekhar announced that MeitY would appoint a nodal officer to oversee platforms' safe harbor status under the IT Rules, 2021. [136]

Intermediaries can separately be held liable for infringing the Copyright Act, 1957, [137] under the law and licensing agreements. [138] A 2012 amendment limited the liability for intermediaries that link users to material copied illegally. The amendment also mandated that intermediaries disable public access for 21 days within 36 hours of receiving written notice from the copyright holder, pending a

court order to remove the link. Intermediaries can assess the legitimacy of the notice from the copyright holder and refuse to comply. [139]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**2**/4

The government has broad authority to order online content blocked or censored, without transparency and limited procedure for appeal.

In February 2021, the MeitY enacted the IT Rules, 2021 (see B2, B6, C4, and C6). [140] Significant social media intermediaries—defined as companies whose platforms host at least five million users—have 36 hours from being notified to remove content that is unlawful, including that which undermines state sovereignty, friendly relationships with other states, security, public order, decency, or morality. [141] Content that shows nudity or is a depiction of a sexual act must be removed within 24 hours of receiving a complaint. [142] Significant social media intermediaries are also required to deploy automated moderation tools to proactively identify and remove offending categories of content, particularly child sexual abuse imagery. [143] When content is removed pursuant to terms of use, the companies must notify users, provide clear reasons for the decision, and offer an avenue for appeal. [144]

Significant social media intermediaries must appoint certain India-based officers. A nodal person of contact is required to coordinate with law enforcement, while a chief compliance officer must comply with takedown orders from a court, government agency, or any other competent authority within 36 hours, and can face potential criminal prosecution under provisions of the IT Act and formerly the penal code. [145]

Separately, social media intermediaries, regardless of their size, must create grievance redressal mechanisms under the Intermediary Rules 2021. A grievance officer must acknowledge complaints about content from any user within 24 hours and resolve them within 15 days. [146] The officer is also responsible for orders issued by competent authorities, courts, or other government agencies. The law also empowers authorities to issue emergency blocking orders but does

not specify time limits for the operation of blocking orders or provide affected parties the right to a hearing. [147]

Additionally, the rules subject digital news media and OTT platforms to a regulation system and a code of ethics. [148] The code instructs content creators to consider whether content affects India's sovereignty, jeopardizes security, or affects friendly relations with foreign countries. [149] OTT platforms are cautioned to consider India's multireligious and multiracial society and be mindful of content that relates to religion and race. [150] A self-regulation body and interdepartmental committee are granted enforcement powers, including recommending that the government block content under the IT Act.

Amendments to the IT Rules passed in October 2022 established rules for GACs, which hear appeals against decisions taken by social media platforms to remove content. The GACs became functional in March 2023. [151] Amendments passed in April 2023 require intermediaries to remove information identified as "fake or false" by a government "fact-checking" unit. The April 2023 amendments also expand the scope of the rules to cover online gaming platforms. [152] Satirist Kumal Kamra challenged the fact-checking provision of the April 2023 amendments before the Bombay High Court on free expression grounds. [153] In response to the lawsuit, the MeitY stated that the provisions would only apply to information about government policies and programs. [154]

The government appointed the Press Information Bureau's fact-checking arm as the "fact-checking unit" in March 2024, [155] leading the Supreme Court to issue a stay on its implementation. [156] In September 2024, after the coverage period, the Bombay High Court struck down the provision, labeling it unconstitutional. [157]

Ambiguity around the rules' definitions and implementation, such as uncertainty as to which entities are considered digital news platforms, has further fueled concern. [158] Over 15 legal challenges have been lodged against the rules, questioning their constitutionality; [159] as of March 2024, the Supreme Court had ordered all cases transferred to the Delhi High Court for a consolidated hearing (see C4). [160] The Bombay and Madras high courts stayed clauses relating to the operation of the code of ethics and the grievance redressal mechanisms in August and September 2021, respectively. [161] The impact of these orders on the rules' information-sharing provisions, which require digital news media publishers to

furnish information about themselves to the MIB, is not immediately clear (see B6). [162]

Blocking of websites takes place under Section 69A of the IT Act and the 2009 Blocking Rules, [163] which empower the central government to direct any agency or intermediary to block access to information when satisfied that it is "necessary or expedient" in the interest of the "sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order, or for preventing incitement to the commission of any cognizable offence relating to above." [164] Intermediaries' failure to comply is punishable with fines and prison terms of up to seven years. [165]

The Blocking Rules apply to orders issued by government agencies, who must appoint a nodal officer to send in requests and demonstrate that they are necessary or expedient under Section 69A. [166] The rules provide an extensive review procedure for blocking requests, including a notice provision to impacted parties and an opportunity for appeal, [167] but provide exceptions for emergencies. [168]

The constitutionality of Section 69A and the Blocking Rules of the IT Act was challenged in the landmark 2015 *Shreya Singhal* case. [169] The Supreme Court upheld the constitutionality of both but read the Blocking Rules [170] to include both the right to be heard and the right to appeal. Blocking orders must provide a written explanation and allow for reasonable efforts to contact the originator of the content for a hearing. [171] However, the rules continue to require that the orders and actions based on them be kept "strictly confidential"; [172] hence, there is no information on the extent of compliance with the judgment.

In November 2023, the Madras High Court ordered Roots Tamil, a YouTube news channel, be restored, resolving a lawsuit over the MeitY's May 2023 blocking of the site. The MeitY contended that the videos on the channels were said to be advocating sectarian sentiments; the petitioner argued that the videos were simply reporting on political speeches. [173]

In July 2022, Twitter, now known as X, filed a lawsuit in the Karnataka High Court challenging removal orders issued throughout 2021 (see B2). The lawsuit contended that the orders rested on an overly broad interpretation of the IT Act.

[174] The court dismissed the lawsuit in June 2023 and criticized the company's delay in complying with the removal orders. [175] In appeal before the Karnataka High Court, X has sought disclosure of the removal orders; a hearing was held in February 2024. [176]

Indian courts can also order content takedowns. [177] Since 2011, courts have blocked content relating to copyright violations through broad John Doe orders, which can be issued preemptively and do not name a defendant. [178] ISPs have occasionally implemented such orders by blocking entire websites instead of individual URLs, regardless of whether the websites were hosting pirated material. [179] For instance, the Delhi High Court ordered the Union government to permanently block access to three websites that deceived individuals with false promises of employment at Tata-owned Croma, an electronics retail chain, in February 2024. [180] The judiciary has noted that John Doe orders can lead to excessive blocking, [181] and civil society has called for greater transparency. [182]

The IT Act and the now-defunct penal code prohibit the production and transmission of "obscene material," [183] but there is no specific law against viewing pornography in India. The Delhi High Court in April 2021 heard a matter where an individual's photographs were taken from private social media accounts and uploaded onto pornographic websites without her consent. It outlined a template for how directions should be issued in similar cases, suggesting that websites or online platforms be obliged to immediately remove the content upon receipt of a court order. It further suggested that search engines should deindex and dereference such content, and proactively monitor for and disable access to identical content, among other recommendations. [184]

There is no legally established right to be forgotten in India, despite several attempts in recent years to codify this principle. [185] But in March 2024, the Madurai bench of the Madras High Court ruled to safeguard the rights to privacy and to be forgotten in a case involving a person acquitted in a sexual assault case in 2011. The court directed the redaction of his name and personal information from the judgment. [186]

Social media platforms' removal of content has lacked transparency and consistency. For example, the *Wall Street Journal* reported in August 2020 that a Facebook executive in India opposed applying the platform's content-moderation

rules to at least one member of the ruling party and several other individuals and groups, due to the platform's business interests. [187] Facebook denied claims of bias and stated that the application of their policies was open, transparent, and nonpartisan. [188]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**3**/ 4

Threats of criminal charges and increased online harassment (see C3 and C7) have reportedly contributed to more self-censorship among both individuals and news outlets, as has the growing influence of the BJP and its recent popular electoral mandates. [189] CSOs have expressed concern that the Intermediary Rules 2021 may also lead to self-censorship by digital media and OTT platforms. [190] Content creators are reportedly wary of increased scrutiny by the government and other stakeholders, particularly in relation to more sensitive topics such as politics and religion. [191]

Journalists and commentators have reported self-censoring in response to increased government pressure on the media. For example, after authorities ordered social media platforms to remove the British Broadcasting Corporation (BBC) documentary *India: The Modi Question* (see B2), some commentators stated that they avoided reporting on the removal. [192] A spate of tax investigations, [193] arrests, and online harassment aimed at media organizations and journalists have also fueled self-censorship. Programs like the MHA-run cybercrime volunteer initiative, which invites ordinary people to report on their peers by flagging "unlawful content" but does not define the term, may also affect online expression. [194]

However, many independent online outlets, individual journalists, and ordinary users, including those from marginalized communities, continue to report on and speak publicly about controversial or political topics. [195]

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	1 / 4

Score Change: The score declined from 2 to 1 because the government has deployed state resources to manipulate online information, while parties, candidates, and prominent officials spread false information about political issues, particularly over the course of the 2024 elections.

Manipulated content spread by domestic actors, including political parties and leaders, permeates the online environment in India, including during the April–June 2024 parliamentary elections. While figures across the political spectrum spread false and misleading information to mobilize support, researchers and journalists have documented how the tactic is disproportionately utilized by the BJP. **196**

Conspiracy theories, rumors, and false and misleading information that depicted India's Muslim community as seeking to undermine Indian national identity or marginalize its Hindu majority spread widely online during the coverage period, including from BJP accounts. According to fact-checking organization BOOM and disinformation researchers India Hate Lab, anti-Muslim hate speech spread online in the year ahead of the elections, much of it linked to narratives that Hindus were under threat from a growing Muslim population. **197** A review published by the London Story, a foundation that studies hate speech, found over 50 instances where official BJP social media accounts used the term "Vote Jihad" to allege electoral coordination between the opposition Indian National Congress and India's Muslim community to undermine the country. **198** (Similar phrases like "love jihad" and "Corona jihad" spread widely online in previous years to associate Muslims with, respectively, conspiracies to cultivate interfaith marriages and spread the COVID-19 pandemic. **199**) A *Washington Post* investigation released in September 2023 found that the BJP and its allies had operated a network of 150,000 workers in the state of Karnataka, who spread progovernment, anti-Congress, and anti-Muslim messages to prospective voters on WhatsApp. The investigation also identified a loose group of online trolls affiliated with the BJP who spread overtly inflammatory content on party-coordinated WhatsApp groups. **200**

Researchers have found that the BJP spread favorable narratives during the elections through networks of accounts that were not clearly affiliated with campaigns or officials. A May 2024 Al Jazeera investigation found that the BJP operated a network of "surrogate" Facebook pages—ostensibly nonpolitical pages purchased by the party to disseminate progovernment talking points without disclosing their political affiliation. According to a BJP worker interviewed by Al Jazeera, "A lot of things that we cannot say, or post, from [the PM's or party's handles], we run them through surrogate pages in Varanasi." [201] In a report released during the April–June 2024 electoral period, researchers at the Tech Transparency Project found an informal market of Facebook users selling accounts on the platform that they claimed were authorized to run political advertisements, citing examples dating back to 2023. [202] Previously, a March 2022 Al Jazeera report found that Jio Platforms exploited a loophole in electoral regulations to promote surrogate advertisements for the BJP on Facebook during the 2019 Lok Sabha elections, and that the party had benefited from how content was promoted via the platform's algorithmic recommendation systems. [203]

False claims relating to the election were spread by other political parties. In April 2024, social media accounts affiliated with the opposition Congress and AAP reposted a doctored video depicting MHA minister Amit Shah saying that the BJP would withdraw social guarantees for scheduled castes. Social media workers affiliated with the accounts were arrested (see C3). [204]

Manipulation campaigns aimed at influencing perceptions of India's policy in Jammu and Kashmir have been linked to the Indian government. In September 2023, the *Washington Post* reported that Facebook's Coordinated Inauthentic Behavior unit had uncovered a large-scale social media influence operation praising the Indian army's actions in Kashmir, operated by the army's Chinar Corps. The network reportedly sought to accuse Kashmiri journalists of separatism and sedition. The network reportedly remained active for a year after Facebook's New Delhi office refused to have it removed, citing concerns about angering the Indian government and potential legal repercussions, including imprisonment. [205] Similarly, in September 2023, the former X head of trust and safety disclosed that the company had linked a network that spread pro–Indian military and anti-Pakistan narratives to the Indian military in 2021, but refrained

from disclosing that link due to fear of retribution from the Indian government. [206]

Efforts to manipulate online content to favor political parties or prominent officials have been reported in previous years. The Facebook Papers, a collection of leaked internal documents from Facebook released in October 2021, [207] revealed that Facebook employees had found that bots and inauthentic accounts tied to the ruling party and opposition figures had potentially affected elections in India, had found that anti-Muslim hate was increasing, and that misinformation was exacerbated by measures aimed at increasing meaningful interaction on the platform. [208] In February 2021, Newslaundry published a report detailing how the "Hindu Ecosystem" group, created by a member of the BJP, spread content supporting them on social media. [209] The report discusses how a network of over 20,000 participants was given content to spread on Twitter at predetermined times to artificially cause certain hashtags to trend. [210]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**2**/3

Online news outlets, blogs, and other publishing platforms were previously not required to register, obtain licenses, or provide information to the state to publish content. However, the Intermediary Rules 2021 imposed new obligations on digital news publishers and OTT platforms to furnish details about their entities to the MIB and provide a monthly report of grievances they have received, along with information about any actions they took in response. [211]

The MIB issued a notification in May 2021 requiring digital news organizations and OTT platforms to furnish the specified information, [212] and later disclosed that over 2,100 such platforms had done so as of January 2022. [213] The IFF said it was unclear if the provisions under which the MIB issued the relevant notifications are operational, since high courts have stayed provisions of the IT Rules that affect digital media organizations and OTT platforms; those cases remained ongoing as of the end of the coverage period (see B3). [214]

The Telecommunications Act, 2023, created an expansive licensing regime that may apply to a broad range of online services, including OTT platforms, though it

had not been implemented as of the end of the coverage period. [215]

The 2019 amendments to the Foreign Direct Investment Policy (FDI Policy) imposed a 26 percent cap for foreign investment in digital media companies, broadly defined as companies that upload or stream news and current affairs through digital media. [216] Digital media platforms were given until October 2021 to comply with the cap. [217] In December 2023, the BBC announced that it would restructure its India operations, instead becoming Collective Newsroom, an organization primarily owned by Indian citizens, to comply with changes in the FDI Policy. This restructuring came after tax officials raided the BBC's Delhi and Mumbai offices in February 2023, following the release of *India: The Modi Question*; the documentary examined whether Prime Minister Modi sufficiently endeavored to stop interreligious clashes in the state of Gujarat in 2002, when he was its chief minister. [218] Separately, the government mandated in 2020 that digital media companies must receive preapproval for foreign investment from certain neighboring countries, including China, and introduced regulatory approvals necessary for the transfer of shares of Indian digital media companies.

The Foreign Contribution (Regulation) Act (FCRA) regulates foreign funding of domestic nongovernmental organizations (NGOs). Since 2014, FCRA regulations have been tightened several times, making it increasingly difficult for NGOs to receive funding. The FCRA licenses of about 19,000 NGOs have been canceled according to a November 2020 report by the International Commission of Jurists, silencing "critical voices" and impeding their ability to conduct their activities online. [219]

The Net Neutrality Rules, adopted in July 2018, are considered among the world's strongest. [220] With only some exceptions, the rules prevent service providers from interfering with content, including through blocking, throttling, and zero-rating. [221]

The government released updates to the Central Media Accreditation Guidelines in February 2022, which outline accreditation terms for journalists and for eligible news sites. The guidelines included a clause on the withdrawal of journalists' accreditation if they act in a manner prejudicial to the country's security, sovereignty, and integrity; friendly relations with foreign states; or public order, or are charged with a serious offense. [222] Press freedom and internet freedom

groups raised concerns that the guidelines could be abused to censor journalists critical of the government. [223] A March 2021 rule that limits holders of the Overseas Citizen of India (OCI) permanent-residency status from working as journalists may also impede news sites. [224]

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	**3**/4

Online media content in India is diverse and debate is lively. While digital divides persist, users can increasingly access local-language content (see A2). [225] At least one estimate claimed that 70 percent of Indian users could access online news in their local language at the end of 2020. [226] Online spaces for the LGBT+ community are growing, [227] and there is some representation of LGBT+ people in mainstream digital advertisements, television, and media. [228] Nevertheless, CSOs noted that LGBT+ people and experiences do not receive proportionate online coverage. [229]

Use of virtual private networks (VPNs) is increasing, enabling people to evade government censorship and access more diverse internet content, [230] though the government has made overtures to limit their use. Directions issued by the Computer Emergency Response Team (CERT-In) in April 2022 required VPN providers to store user data, leading to some providers withdrawing servers from or restricting services in India (see C4). In 2021, the Parliamentary Standing Committee on Home Affairs recommended that the government ban the use of VPNs on the grounds that it allows criminals to remain anonymous online (see B1 and C4). [231] However, this proposal has been criticized for having the potential to violate privacy rights, security, net neutrality, and internet access, as well as for being unlikely to deter criminal activity online. [232]

Misinformation about the conflict in Manipur circulated widely during the crisis (see A3). [233] For example, videos alleging rape of Meitei women by Kuki men have incited violent reprisals, resulting in targeted sexual violence against Kuki women. Journalists and media commentators in Manipur noted that biased news coverage had hampered accurate information gathering and reporting. [234]

False information and doctored videos have led to offline violence. [235] According to one tally, at least 31 people were reportedly killed in India between 2014 and 2018 in connection to rumors spread on WhatsApp, often about child kidnappings. [236]

Increasing media polarization, which also undermines access to reliable information online, has been on the rise in the last decade. News outlets and commentators that criticize the government face the risk of politicized government intervention, such as tax raids. [237] In November 2022, NDTV, then one of India's last independent news media organizations, was bought by Gautam Adani, a long-standing ally of Prime Minister Modi, raising concerns over the organization's continued independence and the status of press freedom in India generally. [238]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**4** / 6

Digital activism has driven important social debates and people have mobilized online around policy changes. For example, in July 2023, environmental activists mobilized online and in person across the country to protest a proposed law that would roll back conservation protections for forests. [239]

However, local authorities have continued to impose internet shutdowns amid protests (see A3) and the government is suspected of targeted activists with invasive spyware tools (see C5). Human Rights Watch (HRW) reported that 43 percent of internet shutdowns between 2020 and 2022 were either to prevent or in response to protests. [240] In February 2024, for example, mobile services were suspended in seven districts of Haryana due to a march called by farmers' unions. [241]

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on	**4** / 6

the internet, and are they enforced by a judiciary that lacks independence?	

The constitution grants citizens the fundamental right to freedom of speech and expression, [242] including the right to gather information and exchange thoughts within and outside India. [243] The right to access information is also recognized as an inalienable component of free expression rights, [244] and press freedom has been read into the freedom of speech and expression clauses. [245] These freedoms can be restricted by law (but not by executive action) in the interests of state security, friendly relations with foreign states, public order, decency and morality, and the sovereignty and integrity of India, as well as in instances related to contempt of court, defamation, and incitement. [246]

The judiciary is independent. Although commentators have argued that the courts show signs of politicization, [247] judgments continue to protect free expression and other constitutional rights in most cases. A 2015 Supreme Court ruling struck down a broad provision of Section 66A of the IT Act that criminalized information causing "annoyance," "inconvenience," or "danger," among other ill-defined categories. Nevertheless, cases continue to be registered under this provision, and the Supreme Court has issued notice requiring high courts to report all cases filed under Section 66A (see C2). Additionally, the court in the *Shreya Singhal* judgment [248] affirmed that free speech online is equal to free speech offline (see B3). [249]

Courts have also addressed the right to internet access. In September 2019, a single-judge bench of the Kerala High Court found that freedom of expression includes access to the internet and internet infrastructure. [250] The Supreme Court's January 2020 *Anuradha Bhasin* judgment placed limits on restrictions to internet access (see A3), [251] although compliance with the decision has been an issue. [252]

However, there have also been instances where the courts have failed to adequately protect citizen rights (see B3). For example, in December 2022, the Supreme Court declined to hear an appeal regarding the use of a journalist's phone contents for the purposes of a law enforcement investigation, hampering the journalist's ability to protect her work and sources. [253]

The Digital Personal Data Protection Act, 2023 (DPDPA), was passed in August 2023 (see C6) and amended the Right to Information Act, 2005, to exempt a greater degree of information about public officials from the transparency law. [254] The proposal had been widely criticized by civil society and the opposition for limiting government accountability efforts. [255]

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**2**/4

Indian law criminalizes certain forms of expression, which are frequently invoked to arrest or imprison people for their online activity on political and social issues (see C3).

In December 2023, Parliament passed the BNS, a criminal code meant to replace the 1860 penal code as part of a broader overhaul of the colonial-era legal framework. The BNS took effect in July 2024, after the coverage period, and carries over most of the criminal penalties previously outlined in old penal code. [256] The BNS excludes the old code's Section 124A sedition clause, which was often used against journalists, but introduces a similar provision that criminalizes attempts to "excite secession or armed rebellion or subversive activities, or encourages feelings of separatist activities or endangers sovereignty or unity and integrity of India." The provision applies to electronic communication and carries a sentence of life imprisonment in severe cases or otherwise up to seven years' imprisonment. [257]

Under the penal code, individuals could have been sentenced to between two and seven years in prison for speech that is found to be seditious, [258] obscene, [259] or defamatory; [260] to promote "enmity between different groups on ground of religion, race, place of birth, residence, language"; [261] is deemed "prejudicial to maintenance of harmony"; [262] or consists of statements, rumors, or reports that may cause fear or alarm, disturb public tranquility, or promote enmity or ill will. [263]

The Official Secrets Act criminalizes communication of information that may have an adverse effect on the sovereignty and integrity of India. [264] The National

Security Act allows the police to detain an accused person for up to one year without charge and has been invoked in relation to speech online. [265]

Section 67 of the IT Act bans the publication or transmission of obscene or sexually explicit content in electronic form, and Section 66D punishes the use of computer resources to impersonate someone else to commit fraud. While the Supreme Court in 2015 struck down Section 66A (see C1) for being vague and overbroad, similar complaints continue to be registered under the provision, as well as under sections 67 and 66D and the colonial-era penal code (see C3). [266] In August 2021, the Supreme Court issued a notice to all high courts to report cases filed under Section 66A, in a case pertaining to the continued use of the provision by law enforcement agencies and the lower judiciary, stating "this cannot continue." [267] In October 2022, the Supreme Court issued fresh directions ordering states to stop prosecuting people on the basis of Section 66A and held that all ongoing Section 66A cases should stand as deleted. [268]

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**2** / 6

People risk being arrested and detained for political, social, and religious speech or other forms of online content authorities deem objectionable or derogatory, especially during major political events.

Journalists were detained for their online posts during the coverage period. [269] For example, in November 2023, Kerala police launched an investigation into journalist Rejaz M Sheeba Sydeek over a report on the Maktoob Media news site involving alleged anti-Muslim bias on the part of that state's police. [270]

In October 2023, Prabir Purkayastha, the founder and editor in chief of news site NewsClick, was arrested by the Delhi police; officers also arrested Amit Chakraborty, the outlet's head of human resources, who later signed a plea deal. Police filed a wide range of charges against Purkayastha and NewsClick under the Unlawful Activities Prevention Act and the penal code, in part over allegations that it received funding from China. Over 40 NewsClick journalists and people affiliated with the outlet were detained or had their homes raided in October 2023, and the office of NewsClick was sealed. [271] A Delhi court granted bail to Purkayastha in

May 2024 after the Supreme Court invalidated his arrest and ordered his release, highlighting that the police had failed to inform him of the grounds for his arrest before detaining him. [272]

Activists and human rights defenders also face arrest for their online activities. In July 2023, an academic and two Kuki activists were summoned by an Imphal court for allegedly supporting a separate state and inflaming communal passions during interviews with the Wire. [273]

People are penalized for publishing or sharing content concerning politicians and religious groups in India, including during electoral periods. In August 2023, Uttar Pradesh police arrested a WhatsApp group administrator over a post made on the group that purportedly disparaged chief minister Yogi Adityanath. [274] In January 2024, Uttar Pradesh officers arrested a man for posting a video containing morphed photographs of several prominent political leaders on social media. [275] In April 2024, Ahmedabad police arrested an INC aide and an AAP party worker after they posted a doctored video of MHA minister Amit Shah on social media; in May, Telangana police arrested five INC workers on similar charges over the same video. [276]

Journalists in Jammu and Kashmir, which is excluded from this report's scoring, frequently face such restrictions on their online activities. In March 2024, Kashmiri journalist Aasif Sultan was arrested two days after his release on bail, marking the third time he has been charged and detained without trial in over five years; the arrests relate to his work for the online outlet Kashmir Narrator. [277] In March 2023, a special National Investigation Agency (NIA) court filed charges of sedition against academic Abdul Aala Fazili and Fahad Shah, editor of the Kashmir Walla. The charges, filed under the UAPA, were brought against the two in relation to an article written by Fazili—titled "The Shackles of Slavery Will Break"—published on the news site in 2011.

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**2**/4

Some laws risk undermining end-to-end encryption and limiting anonymity online. Prepaid and postpaid mobile customers have their identification verified before

connections are activated. [278] There is a legal requirement to submit identification at cybercafés [279] and when subscribing to internet connections.

Under the Telecommunications Act, 2023, [280] the government may prescribe rules requiring telecommunications service providers to use "verifiable biometric based identification" to identify its users. [281] The act specifically restricts users from providing any false information, "suppress[ing] any material information, or [to] impersonate another person" while obtaining services. [282] While these measures are aimed at protecting users, this may further decrease the possibility of anonymous online communications.

Other provisions of the Telecommunications Act pose a potential threat to end-to-end encryption. The act grants the government authority to establish standards and conformity assessments for encryption technologies. Emergency powers and a requirement to disclose communications in "an intelligible format" may be used to compel decryption and monitoring of private communications, and no exceptions have been provided for end-to-end encrypted communications. [283] Such measures raise significant concerns regarding privacy and surveillance. [284]

The Intermediary Rules 2021 impose certain restrictions for anonymity and encryption, [285] though it appears that the government has not enforced some of those measures. [286] Significant social media intermediaries must allow users to "voluntarily" verify their accounts, including through phone numbers, and clearly mark which users have done so. Digital rights organizations have expressed concerns that this verification could be made mandatory in the future. [287] The rules also require that significant intermediaries be able to identify the first originator of information if requested by a competent authority or court in certain cases related to public order, sexually explicit or child abuse material, and India's sovereignty, integrity, and security. [288] Technical experts have raised concerns that such traceability is not possible without breaking end-to-end encryption, [289] as this would require the intermediaries to track every message being sent over the platform, [290] despite the government's claim that it did not intend to undermine the technology. [291] The government released a list of frequently asked questions on the Intermediary Rules in November 2021, which stated that the intent of the rule on identifying the first originator of a message was not intended to break or weaken encryption. [292]

In May 2021, WhatsApp sued the government in the Delhi High Court, arguing that the message traceability provisions of the IT Rules violated the right to privacy. [293] The government reportedly filed an affidavit arguing that WhatsApp—as a foreign company with no local entity—could not claim any fundamental rights on behalf of users, or challenge the constitutionality of an Indian law. [294] In April 2024, WhatsApp informed the Delhi High Court it would end service provision in India if compelled to break encryption, in a separate case over the IT Rules traceability provision. [295]

In May 2023, an inauthentic resignation letter with a forged signature of a chief minister sparked a legal battle in Tripura, prompting the state police to invoke the IT Rules traceability provision to trace its origin on WhatsApp. It was the first time an Indian law enforcement agency invoked this provision against WhatsApp. After a local court granted the request to track down the originator, WhatsApp approached the Tripura High Court in September 2023, which granted a stay on the traceability order. [296]

In August 2024, after the coverage period, a Delhi High Court ordered the Wikimedia Foundation to identify three of its anonymous contributors. The order was issued in a defamation case that news agency Asian News International filed over the contents of a Wikipedia page about the agency. [297] In September 2024, the High Court judge threatened to block Wikipedia if it does not comply. [298]

In April 2022, the CERT-In issued a set of directions under the IT Act requiring cloud service providers and cryptocurrency exchanges to log user data for five years. [299] While the use of VPNs remained legal, VPN providers must store users' names, addresses, contact numbers, period of subscription, email and IP addresses, and the purpose of using their services. [300] Companies have argued that logging such information would violate their users' privacy and may also be technically unfeasible. [301] Clarifications on the rules issued in May 2022 clarify that the provisions would not be applicable to corporate and enterprise VPNs. [302] The directions, which came into force on September 2022, have led several VPN providers such as Proton VPN, NordVPN, Surfshark, ExpressVPN, and IPVanish to withdraw their servers from India; [303] others, including TunnelBear, announced their services would no longer be available to users in India.

ISPs setting up cable-landing stations are required to install infrastructure for surveillance and keyword scanning of all traffic passing through each gateway under 2014 rules. [304] The ISP license bars providers from deploying bulk encryption; restricts the level of encryption for individuals, groups, or organizations to a key length of 40 bits; [305] and mandates prior approval from the DoT or a designated officer to install encryption equipment. [306]

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

In August 2017, a landmark Supreme Court ruling affirmed privacy as a fundamental right embedded in the right to life and liberty, and intrinsically linked to other fundamental rights like free expression. [307] State surveillance can nevertheless infringe on this right, [308] and private companies offering spyware or hack-for-hire services have flourished. [309]

The existing surveillance architecture concentrates surveillance powers in the executive branch of the Union government and does not provide for meaningful oversight or review, either judicial or parliamentary, of surveillance activities. [310] Communications surveillance may be conducted under the Telegraph Act [311] and the IT Act [312] to protect defense, national security, sovereignty, friendly relations with foreign states, public order, and to prevent incitement to a cognizable offense. Section 69 of the IT Act broadly allows surveillance for "the investigation of any offense." [313] The Telegraph Act is being replaced by the Telecommunications Act, which was passed in December 2023. The new law retains the broad powers for telecommunications interception, lacking oversight and avenues for redress (see C4). [314] In September 2024, after the coverage period, the Ministry of Communications released implementing guidelines relating to telecommunications interception. [315]

Currently, the home affairs secretary at the central or state level issues interception orders based on procedural safeguards established by the Supreme Court and the Telegraph Act. [316] These orders are reviewed by a committee of government officials. [317] Interception orders are limited to 60 days, and renewable for up to 180 days. [318] In emergencies, phone tapping may take place

for up to 72 hours without clearance; records must be destroyed if the home secretary subsequently denies permission. [319]

The Indian government is also reported to operate several different technical systems for surveillance in the interests of national security and law enforcement. The Central Monitoring System (CMS) reportedly allows government agencies to intercept any online activities, including phone calls, text messages, and Voice-over-Internet-Protocol (VoIP) communication. [320] A petition filed by the Centre for Public Interest Litigation (CPIL) and the SFLC in December 2020 argued that CMS and two other programs (the surveillance software Network Traffic Analysis [NETRA] [321] and the integrated National Intelligence Grid [NATGRID]) should be discontinued because they allow bulk surveillance and data collection. [322] The case remained pending during the coverage period. [323] In February 2021, the MHA in an affidavit before the Delhi High Court claimed that agencies are not granted "blanket permission" for surveillance; that surveillance programs are necessary to monitor "terrorism, radicalization, cybercrime, [and] drug cartels"; [324] and that there is sufficient oversight on such surveillance activities. [325]

The Indian government is suspected of using sophisticated spyware technology. In October 2019, WhatsApp claimed that Pegasus software from the Israeli NSO Group was used to spy on at least two dozen activists, lawyers, academics, and journalists in India in May 2019. [326] In July 2021, Amnesty International and Forbidden Stories reported that more than 1,000 phone numbers in India—including those belonging to politicians with the Congress party, activists, journalists, public health experts, and Tibetan exiles—appeared in a leaked data set of possible Pegasus targets. [327] While it is unclear how many phones were targeted by Pegasus, preliminary reporting indicates that the spyware infiltrated the devices of at least 149 people in India. [328] In October 2023, several Indian opposition leaders and journalists, including MPs from various parties, reportedly received warning messages from Apple indicating they may have been targeted by "state-sponsored attackers." [329] Anand Mangnale, partner journalist at the Organized Crime and Corruption Reporting Project, was reportedly targeted by Pegasus within hours of sending prepublication questions to the Adani Group, India's largest business conglomerate, as part of an investigation. [330]

Government officials responded by questioning the reliability of Apple's internal threat algorithms and launching a CERT-In inquiry into the security of Apple

devices, [331] and pressed Apple to retract the warnings. [332] As of April 2024, Apple appeared to have dropped the term "state-sponsored" from its threat notification policy. [333]

While the NSO Group claims to only work with state agencies, government officials have repeatedly denied purchasing its software. [334] However, when questioned about the claims, the MHA minister in November 2019 argued that Section 69 of the IT Act and Section 5 of the Telegraph Act allow certain authorities to intercept, monitor, or decrypt "any information from any computer resource" in the country. [335] The IFF has reported that state investigations into the hack remain confidential. [336]

In August 2022, a panel convened by the Supreme Court in October 2021 submitted its report following an independent probe into claims that the government used Pegasus. The Supreme Court noted that the government did not cooperate with the investigation. [337] As of April 2024, the report had not been publicly released, though the court has stated that it plans to do so. [338]

In March 2023, the *Financial Times* reported that the Indian officials were seeking spyware tools from companies with a lower profile than the NSO Group. [339] Separately, Citizen Lab and Amnesty International reported finding evidence that at least nine academics, lawyers, writers, and activists were targeted between January and October 2019 in a spear-phishing campaign to install the spyware NetWire. [340] The targeted individuals included human rights defenders calling for the release of activists arrested for allegedly participating in protests and violence in Maharashtra, known collectively as the BK16, including prominent activists Rona Wilson and Anand Teltumbde. [341] In February 2022, cybersecurity firm SentinelOne attributed the campaign to a threat actor dubbed ModifiedElephant, which allegedly planted fabricated evidence on the personal devices of the BK16. [342] Subsequent reporting linked police in Pune to ModifiedElephant. [343]

The government uses the Aadhaar national biometric database for the provision of multiple public services, including food aid, various scholarships, and employment schemes. [344] The system's use poses concerns regarding data privacy and security. [345] In October 2023, US security firm Resecurity reported that the personal information, including information from Aadhaar, of 815 million people had appeared on the dark web. [346] In January 2024, another digital

security firm, CloudSEK, reported that the Aadhaar-linked information of 750 million people had been put up for sale. **347**

In September 2018, the Supreme Court set limits on Aadhaar's use. **348** The ruling held that it was legitimate for the program to be mandatory for welfare schemes and that Indians must link their Aadhaar number to income tax filings and permanent account numbers, but that it cannot be required for services such as obtaining a SIM card, opening a bank account, and receiving educational grants. Despite this, Parliament passed in July 2019 the Aadhaar and Other Laws (Amendment) Bill, **349** which CSOs argue ignored the Supreme Court ruling. **350** As of the end of the coverage period, a case challenging the law was pending in the Supreme Court. **351** The court has also directed that a larger bench review the 2018 judgment, but the bench has not yet been constituted. **352**

In March 2020, it was reported that the government planned to build a database called the National Social Registry that will use data from Aadhaar **353** and capture a vast amount of other personal information, including individuals' marital status, financial status, and property owned. **354** Critics, including Manorajan Kumar, the civil servant who first proposed the National Social Registry, have expressed concerns about privacy and potential data manipulation arising from the system's envisioned implementation. **355** In October 2022, the *Economic Times* reported that the central government was aiming to include caste-census data in the registry. **356**

Police also conduct manual searches of electronic devices often without following the prescribed procedural guidelines. **357** In October 2023, during the raids on NewsClick's office, police seized 250 electronic devices, including hard disks, mobile phones, and laptops belonging to journalists associated with the organization, contributors, and former employees (see C3). **358**

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**2**/6

Technology companies are required to collect extensive personal data, and a variety of laws provide government agencies the ability to access this information.

Ten separate intelligence bodies are authorized to issue surveillance orders to service providers. **359** Online intermediaries are required by law to "intercept, monitor, or decrypt" or otherwise provide user information to officials. **360** The Telegraph Act levies civil penalties or license revocation for noncompliance, **361** and violations of the IT Act can lead to a maximum 10-year jail term. **362** Unlawful interception is punishable by a lesser sentence of three years. **363** Similar provisions are carried in the new Telecommunications Act (see C5). **364**

The IT Rules 2021 changed the way companies must share information with government agencies in certain circumstances. The rules require intermediaries to provide the government with data within 72 hours of receipt of a written order to verify identity, or for the prevention, detection, investigation, or prosecution of offenses under domestic law. **365** The rules also impose new data-retention policies requiring intermediaries to store information for 180 days. **366**

India does not have a data-protection law in force. Rules issued in 2011 under the IT Act provided for greater protection of personal data handled by companies, **367** but do not apply to the government. In August 2023, Parliament passed the DPDPA. The DPDPA was criticized for various provisions that failed to sufficiently safeguard personal data. These include provisions such as the deemed consent clause, which allows for nonconsensual processing of data, and the exemptions clause, which grants wide exemptions from the application of the draft bill to state and private actors. **368** The law will come into effect once the rules framed thereunder are promulgated. **369**

The DPDPA departs from the Data Protection Bill, 2021, which was introduced in December 2021 to replace the earlier Personal Data Protection Bill, 2019, and subsequently withdrawn in August 2022. The DPDP Act dilutes the role of the Data Protection Board, which is not independent and performs only an adjudicatory function, compared to the regulator under the 2021 draft. The 2021 bill mandated data localization; the DPDPA allows for cross-border data transfer. However, the government can restrict the flow of data to specific countries if required. **370**

The telecommunications license agreements require service providers to guarantee the designated security agency or licensor remote access to information for monitoring; **371** ensure that their equipment can provide for

centralized interception and monitoring; and provide the geographic location of any subscriber at a given point in time. **372** Standard Operating Procedures for Lawful Interception and Monitoring of Telecom Service Providers, regulations issued in 2014, **373** restricted interception to a service provider's chief nodal officer, and mandated that interception orders be made in writing. **374** A 2011 Equipment Security Agreement requires operators to develop the capacity to pinpoint any customer's location within 50 meters. **375**

In December 2021, the DoT extended the requirement for telecommunications providers to retain call data and internet usage records of subscribers from one year to two years. **376** In March 2020, news reports revealed that telecommunications companies had raised concerns with the DoT over the bulk call data records sought by the government. **377** Through information requests, the IFF found indications that the records were potentially sought for use cases beyond quality assurance, as the government claimed. **378**

Between July and December 2023, Meta received 91,907 total requests from Union and state governments for user data, an increase from 70,612 requests between January and June 2023. The company produced information for 72 percent of requests received from July to December 2023 and for 68.7 percent of requests received from January to July 2023. **379**

In early 2023, the BJP launched the Saral app to connect with its followers across the country. Saral collects extensive personal and demographic information. Critics raised concerns about undue influence and misuse of government resources in election strategies. According to them, this data, gathered through collaboration between government and party machinery, can enable voter profiling, targeted campaigns, and manipulation of election outcomes. **380**

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**2**/5

Online journalists and commentators sometimes face violent retribution for their work. Online harassment is common and sometimes coordinated, including in line with anti-Muslim conspiracy theories (see B5).

People sometimes face physical violence as a result of their online activities, including while covering the 2024 elections. In February 2024, journalist Nikhil Wagle was attacked by BJP and Shiv Sena workers at four different locations while traveling to an event in Pune. Wagle had posted on social media criticizing Prime Minister Modi and LK Advani, a prominent BJP leader. Despite being aware of the threats against Wagle, the Pune police unofficially detained him for four hours before the event after a First Information Report was filed against him, and the BJP Pune unit threatened to disrupt the event if he spoke. [381] In May 2024, journalist Raghav Trivedi of the news site Molitics was beaten while investigating allegations that women had been paid to attend a BJP rally in Uttar Pradesh; he was reportedly attacked by BJP activists after Trivedi said he had recorded interviews with the women. [382]

In August 2023, the home of Khushboo and Nadeem Akhtar, who run the YouTube news channel Pal Pal News, was set on fire. The Akhtar siblings, who have received death threats for their reporting on violence and discrimination against Muslims, believe the arson attack was connected to their work. [383]

Abuse and trolling are worse when the victim is a woman, is an adherent of a minority religion, is from a lower caste, or otherwise identifies within a marginalized group. [384] For example, television journalist Haseena Shaik faced violent and misogynistic online harassment in January 2024 over a video in which she attended a bicycle rally and rode a bicycle with an Andhra Pradesh minister; much of the harassment came from Telugu Desam Party leaders and supporters. [385] Media outlets have reported widespread online harassment and trolling of investigative journalist Rana Ayyub in response to her work, [386] including politicized investigations. [387]

Social media accounts, some of them affiliated with Hindu nationalism, promote anti-Muslim sentiment and harass perceived transgressors, particularly interfaith couples. For example, fact-checking site Alt News in a February 2024 article identified one case which a prominent anti-Muslim meme page regularly doxed Hindu women involved with Muslim partners, leading to offline harassment and threats. [388] Similarly, in January 2022, Al Jazeera reported on the Bulli Bai app, which reportedly used photographs and deepfakes of prominent Indian Muslim woman journalists and ordinary women to “auction” them online. [389]

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**2**/3

India remained a frequent target of cyberattacks during the coverage period, some of them originating from foreign actors.

Foreign hackers frequently target Indian companies and government agencies, some of them from state-linked groups. A June 2024 report from cybersecurity firms Recorded Future and SentinelLabs identified a Chinese state-backed hacking group as the likely perpetrators of a 2022 attempt to compromise the health data of All India Institute of Medical Sciences patients. **390** In May 2024, cybersecurity firm BlackBerry Ltd. attributed a string of attacks against Indian government agencies and military contractors during the coverage period to a Pakistani state-backed group. **391** State-backed attacks originating from Iran have reportedly targeted Indian government systems in previous years. **392**

According to monitoring by CloudSEK, attacks against Indian government agencies doubled from 2021 to 2022. **393** For example, the hacktivist group DragonForce Malaysia coordinated attacks against government and BJP websites in June 2022 after a prominent BJP official made disparaging remarks about the prophet Muhammad. **394** During the Group of 20 (G-20) summit hosted in New Delhi in September 2023, India's official summit website faced distributed denial-of-service (DDoS) attacks. **395**

The IT Act is the primary legislation governing cybersecurity, and lays out penalties for damaging computers and computer systems. **396** The IT Act penalizes hacking, introducing malware, and DDoS attacks that result in significant damage or disruption to essential services. **397** The law also allows the government to define resources as "critical information infrastructure." **398**

The April 2022 CERT-In directive (C4) also requires all service providers, intermediaries, data centers, companies, and government organizations in India to report cybersecurity incidents within six hours. **399** The government exempted the CERT-In from the purview of the Right to Information Act in November 2023,

raising concerns about transparency. [400] The move came after the regulatory body was tasked with investigating Apple's security notifications regarding "state-sponsored" attacks. [401]

Footnotes

1 Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators 2023-2024," August 14, 2024, https://www.trai.gov.in/sites/default/files/Report_14082024.pdf

2 "Digital 2024: India," DataReportal, February 21, 2024, https://datareportal.com/reports/digital-2024-india

3 "Unstarred Question No. 5379", Lok Sabha, April 5 2023, https://sansad.in/ls/questions/questions-and-answers.

4 "Performance Indicators Reports," Telecom Regulatory Authority of India, https://trai.gov.in/release-publication/reports/performance-indicators-....

5 Speedtest, "Speedtest Global Index", accessed Feb 2024, https://www.speedtest.net/global-index/india.

More footnotes

On India

See all data, scores & information on this country or territory.

See More ›

Country Facts

Population

1,417,170,000

Global Freedom Score

66 /100 **Partly Free**

Internet Freedom Score

50 /100 **Partly Free**

Freedom in the World Status

Partly Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2024

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org

@2024 FreedomHouse