Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**424**
Land:	Indien
Kilde:	Freedom House
Titel:	Freedom on the Net 2021: India
Udgivet:	21. september 2021
Optaget på baggrundsmaterialet:	25. februar 2022

Freedom House

FREEDOM ON THE NET 2021

India

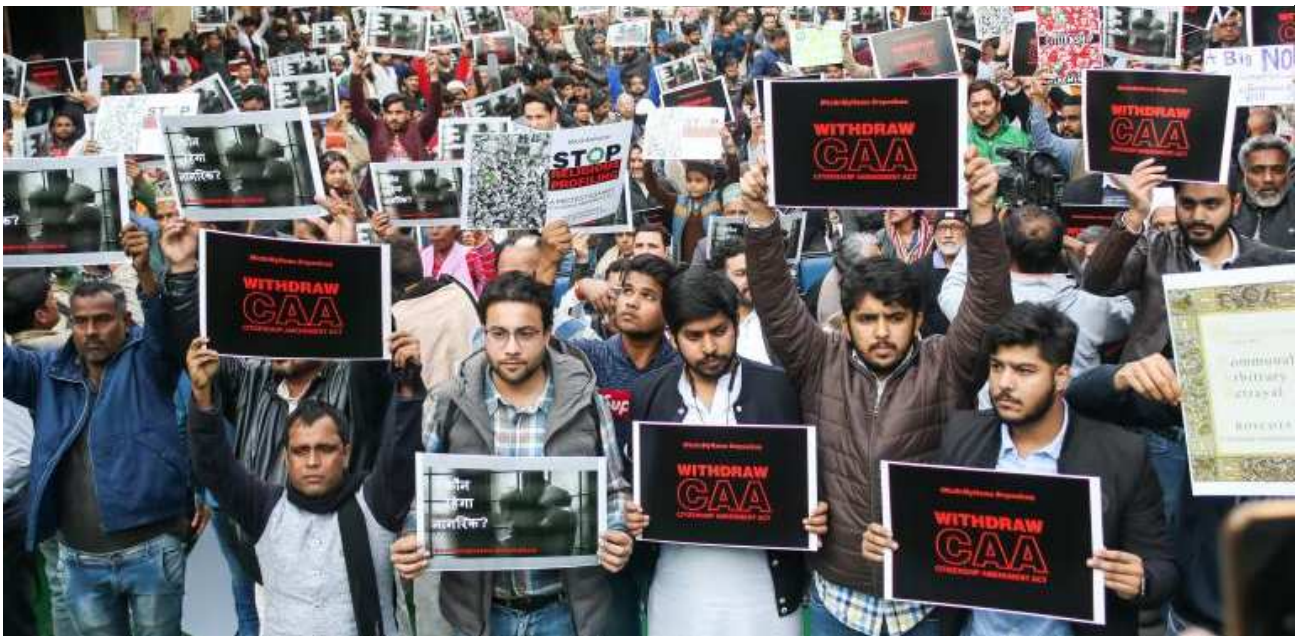
PARTLY FREE

49
/100

A. Obstacles to Access	11 /25
B. Limits on Content	21 /35
C. Violations of User Rights	17 /40

LAST YEAR'S SCORE & STATUS
51 /100 **Partly Free**

Scores are based on a scale of 0 (least free) to 100 (most free)



Overview

Internet freedom in India weakened for a fourth straight year. The contentious new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 imposed broad obligations on large social media companies to further moderate online content, undermine end-to-end encryption, and increased retention of personal data. It also mandated that digital news media and streaming services adhere to a new Code of Ethics that in part serves to guard against purported threats to sovereignty and national security. Government authorities imposed blocks on over 100 apps owned by China-based companies beginning in June 2020, and continued issuing internet shutdown orders, particularly in the context of protests by farmers against new agricultural laws. During the protests as well as during the country's deadly second wave of COVID-19 in April 2021, officials requested US-based tech companies take down content criticizing authorities, shared by opposition figures, journalists, activists, and ordinary users. Meanwhile, civil society and a consortium of news outlets reported on intrusive spyware campaigns that further erode privacy rights. Positively, both governmental and nongovernmental entities continued efforts to bridge the country's digital divides.

While India is a multiparty democracy, the government led by Prime Minister Narendra Modi and the Bharatiya Janata Party (BJP) has presided over discriminatory policies and increased violence affecting the Muslim population. The constitution guarantees civil liberties including freedom of expression and freedom of religion, but harassment of journalists, nongovernmental organizations (NGOs), and other government critics has increased significantly under the current regime. Muslims, scheduled castes (Dalits), and scheduled tribes (Adivasis) remain economically and socially marginalized.

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.*

Key Developments, June 1, 2020 - May 31, 2021

- The Indian government continued to impose frequent internet shutdowns, justified by authorities for reasons including the need to counter disinformation, maintain public safety, prevent communal violence, and curb cheating on exams. Authorities shut off the internet repeatedly amid protests by farmers against agricultural reforms (see A3 and B8).
- Between June and September 2020, following military clashes along the Indian-Chinese border, the government blocked over 100 mobile apps owned by China-based companies, including TikTok and WeChat (see A3).
- During the farmers' protests, and during the second wave of the COVID-19 pandemic, the government ordered social media platforms to take down online content shared by journalists, opposition figures, and ordinary users that criticized authorities (see B2).
- In February 2021, the government released the contentious Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, regulating a broad swath of social media companies, content hosts, and digital media outlets. The rules include new content-removal obligations, in-country representative and reporting requirements, message traceability mandates, and new data-retention rules. Several legal challenges against the measures were filed by the end of the coverage period (see B3, B6, C4, and C6).
- New reports from civil society groups and a consortium of news outlets found more evidence that the government has access to and deploys sophisticated spyware technology like NSO Group's Pegasus and NetWire, including against activists, journalists, lawyers, and opposition figures (see C5).

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**3**/6

India has the second-largest number of internet subscribers in the world after China, having overtaken the United States in 2016. [1] Official statistics listed almost 795.2 million subscribers in December 2020, though only 25.5 million had wired internet connections. [2]

While access is expanding, the rate of internet penetration among India's nearly 1.4 billion residents remains relatively low, reaching 58.51 percent in December 2020 [3] — though that was up from 54.2 percent in December 2019. [4] Of subscribers, 96.7 percent of them access the internet through mobile devices. [5]

India's average connection speed as of July 2021 was among the lowest in the world, at 17.77 megabits per second (Mbps) for mobile internet. Broadband internet ranked much higher but was still considerably below the global average, at 60.06 Mbps. [6]

The Economist Intelligence Unit's Inclusive Internet Index 2021 ranks India 77 out of 120 in terms of availability of the internet, as determined by the quality and breadth of available infrastructure. [7] The World Economic Forum's Global Competitiveness Report 2020 scored India at 72.6 on a 100-point scale for infrastructure that can broaden access to electricity and ICT, below the global average of 78.7. [8]

A number of ambitious public- and private-sector initiatives to improve access to the internet continue. In December 2020, the Prime Minister's Wi-Fi Access Network Interface (PM-WANI) scheme was approved, under which the government will set up a nationwide network of free-of-charge, public Wi-Fi hotspots. [9] [10] In 2016, the public-sector company RailTel launched a project, originally with technical support from Google up until February 2020, to provide free Wi-Fi services at a minimum of 100 railway stations. [11] RailTel plans to work toward providing free Wi-Fi services at more than 5,600 stations. [12]

Launched in 2011, the government's BharatNet project has aimed to provide broadband connectivity to all the 2.5 lakh Gram Panchayats (units of local self-governance at the village level) in India, although the project has faced several delays and challenges (see A2). [13]

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?	**1** / 3

While mobile data plans in India are quite cheap, digital divides remain across geography, language, and gender.

According to a 2021 report from the British-based company Cable, the average cost of one gigabyte of data in India is $0.68. [14] According to the Inclusive Internet Index 2021, India slipped two spots from the previous year and currently ranks 20 out of 120 countries surveyed in the affordability index, defined by cost of access relative to income and the level of competition in the internet marketplace. [15] Similarly, the 2020 Affordability Report released by the Alliance for Affordable Internet ranked India 11 out of 72 low and middle-income countries for affordable and meaningful access, a measure that includes cost, market competition, and public access to the internet as factors. [16]

Internet penetration in rural areas is significantly lower than in urban areas. Rural areas have only 34.6 internet subscribers per 100 people, compared with 104.0 per 100 in urban areas. [17] Several initiatives aim to narrow the urban-rural divide. The government's Digital India Programme, launched in 2014, [18] aims to extend fiber-optic cables to more rural areas, establish internet-connected common service centers (CSCs), [19] and provide residents with e-literacy programs. [20] The program has also proposed using satellites, balloons, or drones to bring faster connections to remote areas. [21]

Until March 2020, the government-led BharatNet project allowed CSCs to provide free internet services in 120,000 locations using a countrywide fiber-optic network. [22] However, after March 2020, the government began charging a fee from users to reduce financial burdens of the project; [23] more broadly, the implementation of BharatNet has faced delays and uneven progress among states. [24] As of May 2021, 62 percent of Gram Panchayats had been connected via fiber-optic cable and made service ready. [25] The deadline for completion of the project was extended to June 2021. [26]

In July 2020, CSCs revealed plans to deploy five-lakh fiber-to-the-home (FTTH) connections to facilitate high-speed internet in villages by year's end. [27] The PM-WANI scheme also aims to provide increased accessibility in rural areas (see A1). [28] Separately, government-run telecom company Bharat Sanchar Nigam Ltd. awarded a contract to Israeli company NovelSat to improve high-capacity satellite and broadband services to remote islands. [29]

With 22 official languages, language remains a barrier to access (see B7). Projects to encourage local-language usage online are underway. As of February 2021, the Dot

Bharat domain was available in all 22 official languages. [30] In December 2020, Google introduced various capabilities to make it easier to use Google services in Indian languages. [31]

There is also a significant gender divide in access to internet, with studies conducted by the Internet and Mobile Association of India (IAMAI) in 2017, 2018, and 2019 [32] finding that only about a third of Indian internet users are women. [33] While research on women's access to and use of mobile services in India has significant gaps, various socioeconomic factors like lower literacy rates and stereotypical notions of the roles of women in society exacerbate the gender divide in access. [34] The divide is particularly stark in rural areas. [35] The National Family Health Survey found that on average less than 3 out of 10 rural women and 4 out of 10 urban women have used the internet. [36] However, the GSMA, a trade body that represents mobile network operators worldwide, noted in its Mobile Gender Gap Report 2021 that the percentage of women who were aware of mobile internet rose from 19 percent in 2017 to 53 percent in 2021. [37] Internet Saathi, a partnership between Google and Tata Trusts, promotes digital literacy among rural women and provides digital skills training to hundreds of women per week in villages. [38] The program had reached over 30 million women by March 2021. [39]

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**1** / 6

Score Change: The score declined from 2 to 1 due to the blocking of over 100 mobile apps owned by China-based companies, including TikTok and WeChat, as well as continued connectivity restrictions throughout the country.

India is a global leader in the number of internet shutdowns imposed, [40] with shutdowns regulated by the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017. [41] During the coverage period, the government also blocked access to social media and communications apps owned by Chinese companies, following heightened tensions along the India and China border.

Local authorities have restricted information and communications technology (ICT) connectivity and usage during times of perceived unrest since at least 2010. [42]

Authorities typically justify shutdowns as cautionary measures required for the maintenance of law and order, to quell potential violence or communal tensions, restrict protests, prevent the spread of disinformation, or to stop cheating on school exams. [43]

The frequency, geographic distribution, and duration of these shutdowns has increased in recent years. In 2020, shutdowns occurred in nine states. As of August 2021, there had been at least 31 instances of internet shutdowns in 2021, including those in Jammu and Kashmir. [44] TopVPN reported that connectivity was throttled for a total of 7,272 hours in 2020. [45]

In January and February 2021, internet access was restricted repeatedly in and around Delhi as farmers protested against controversial agricultural bills (see B8). [46] For example, on January 26, 2021, the internet was reportedly restricted for 12 hours in several of the city's districts, [47] to "maintain public safety and avert public emergency." [48] The shutdown affected more than 50 million mobile subscribers in the area. [49] Similarly, the Haryana State government initially suspended internet services in three districts in the state for more than 72 hours, [50] and then extended the shutdown to 17 of the 22 districts. [51] Previously, in late 2019 and early 2020, during the course of large-scale protests against the controversial Citizenship Amendment Act (CAA), a number of network shutdowns were also reportedly imposed across the country. [52]

In November 2020, the state government of Arunachal Pradesh reportedly temporarily restricted internet services in 15 out of 25 districts to prevent cheating during the state civil services examinations. [53] Amid protests by the Gujjar community demanding reservations in jobs in the Rajasthan government, state authorities reportedly ordered internet shutdowns in October [54] and November of 2020. [55]

In the Jammu and Kashmir region, which is excluded from this report's scoring criteria (see Overview), the state administration repeatedly ordered restrictions on internet services during the coverage period. [56] Earlier, between August 2019 and January 2020, the government of Jammu and Kashmir ordered the longest internet shutdown in India—a total of 213 days—in the wake of the central government's abrogation of Article 370 of the Indian Constitution, which provides special status to the state. [57] Access to 2G networks was restored in January 2020, and 3G and 4G networks were

restored in Ganderbal and Udhampur districts in August 2020. [58] In February 2021, 17 months after the internet services were originally shut off, 4G internet services were restored in Jammu and Kashmir. [59] However, additional short-term restrictions continued throughout the end of the coverage period. [60]

During the coverage period, the government blocked over 100 mobile apps owned by China-based companies, citing concerns over national security and the country's sovereignty. [61] In June 2020, following military clashes along the Indian-Chinese border, the Ministry of Electronics and Information Technology (MeitY) initially banned and the Department of Telecommunication (DoT) ordered internet service providers (ISPs) to block 59 apps, including TikTok, WeChat, and Helo, under Section 69A of the IT Act. The ministry stated that the apps were detrimental to the sovereignty and integrity, defense, and security of India, as well as to public order (see B2). [62] In January 2021, MeitY announced that blocks on 59 of the apps would become permanent, [63] reportedly stating that the companies' responses to government complaints about legal compliance and privacy were unsatisfactory. [64]

In September 2020, the government banned a further 118 Chinese mobile apps, [65] citing reports that the unauthorized transmission of user data to servers located outside India was detrimental to India's national security. [66] In November 2020, another 43 apps were banned, including popular gaming website PUBG. [67]

Most of India's internet infrastructure is privately owned by service providers, thus the government relies on legislative and statutory mechanisms to order shutdowns. Orders to restrict connectivity have usually been justified under Section 144 of the Code of Criminal Procedure, 1973 (CrPC), which permits state actions to maintain law and order. [68] The Gujarat High Court upheld the use of this law to order shutdowns in September 2015, [69] and the Supreme Court refused a petition challenging it in early 2016. [70] However in 2020, the Supreme Court observed with respect to the Gujarat High Court judgement that "the position has changed since 2017, with the passage of the Suspension Rules under Section 7 of the Telegraph Act." [71] Some experts have suggested that this decision implies that Section 144 can no longer be utilized to authorize shutdowns. [72]

Section 69A of the Information Technology Act, 2000 (IT Act) permits the central government to order content takedowns on the internet, while Section 5 of the Indian

Telegraph Act, 1885 (Telegraph Act) allows state and central authorities to order any message to not be transmitted in public emergencies. [73]

In August 2017, the DoT issued new rules, called the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, under the Telegraph Act to regulate the temporary suspension of telecom services. [74] The rules authorize only national- or state-level officials of a certain rank to issue temporary suspension orders to shut down telecommunications services in times of public emergency or when there is a threat to public safety, [75] and mandate that each order should contain reasons for shutdowns to be forwarded to a review committee for assessment. [76] However, several shutdown orders imposed since 2017 were issued under Section 144 of the CrPC by officials not designated under the Telegraph Act rules. [77] Civil society groups have raised concerns that some orders were therefore not issued by authorized officials and lacked the necessary procedural safeguards and checks. [78] In November 2020, the government amended the rules to specify that an order for a shutdown could not be in effect for more than 15 days, but such orders could be renewed. [79] 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. [80]

Courts have directly ruled on the legality of connectivity restrictions. The Gauhati High Court ordered the government of Assam to restore mobile internet connectivity eight days after the state administration shut down the internet indefinitely during CAA protests in December 2019. [81] As of July 2020, another case, involving a 5-day shutdown in May 2020 that affected West Bengal, remained under challenge in the Calcutta High Court for being issued under Section 144 of the Criminal Procedure Code (CrPC) rather than the 2017 Act rules. [82]

In January 2020, the Supreme Court responded to the months-long internet shutdown in Jammu and Kashmir, ruling that the administration of Jammu and Kashmir must review existing shutdown orders in the region. [83] It further ruled that connectivity restrictions across the country should be well reasoned, proportionate, temporary, and present the least restrictive alternative, and that the order should be made publicly available (see C1). [84] However, critics argued that the ruling failed to address the fundamental issue of deprivation of essential services. [85] A related decision in May 2020 [86] reiterated the mandate for a special committee comprised

of state and central government officials to review the orders, [87] but a suit filed in June 2020 alleged that the government had failed to implement the ruling. [88]

Compliance with the Supreme Court's ruling remains unclear. In October 2020, the Gujarat State government refused a right-to-information request from the Internet Freedom Foundation (IFF) to furnish orders about a shutdown publicly, despite the Supreme Court requiring it. [89] Similarly, the organization could not find orders of shutdowns in Rajasthan, [90] Madhya Pradesh, Meghalaya, West Bengal, and Uttar Pradesh on the respective government websites. [91]

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 mobile and internet connections, but fees to enter the market have served as an economic barrier for some providers. As of December 2020, there were 396 operational ISPs in India, [92] up from 358 in 2019. [93] The largest service provider, Reliance Jio, has almost 52 percent of the market, and the top three ISPs together control nearly 95 percent of the market. [94] There are six wireless service providers, [95] with the largest provider controlling nearly 35 percent of the market and the top three operators together controlling over 89 percent of the market. [96] In April 2020, Facebook invested $5.7 billion in a 9.9 percent stake in Reliance Jio. [97] In July 2020, Google announced that it will invest $4.5 billion in Jio Platforms (the owner of Reliance Jio), buying a 7.7 percent stake in the company, and the purchase was approved by the Competition Commission of India (CCI) that November. [98]

A universal license framework, for which guidelines were published in November 2014, [99] reduced legal and regulatory obstacles by combining mobile phone and ISP licenses. Licensees pay a high one-time entry fee, a performance bank guarantee, [100] and annual license fees adjusted for revenue. [101]

In October 2019, a Supreme Court order provided clarity on the percentage of revenue that license holders are required to pay the government—an issue that was contested by the telecom industry for several years. The order mandates that the percentage is calculated on the basis of the entire revenue of the license holder, and

not just revenue from telecom services. [102] Previously, the court rejected petitions from telecom operators requesting a review of the order, [103] and in September 2020, it passed an order which gave 10 years to telecom companies to pay their dues. [104] Both Vodafone Idea and Bharti Airtel are expected to pay millions in overdue fees, raising concerns over their financial stability and the impact on the telecom market. [105]

Over the last decade, there has also been a sharp drop in the number of cybercafés in India, [106] particularly due to the increase in use of smartphones and mobile internet. [107] In 2011, the Indian government introduced rules under Section 79 of the IT Act that imposed multiple licensing and monitoring requirements on cybercafés. [108] Critics said the rules were "poorly framed" [109] with unclear noncompliance penalties and patchy enforcement.

Roughly 15 submarine cables connect India to the global internet, [110] most of which are consortium-owned. [111] There are at least 15 landing stations where the cables meet the mainland, spread across five cities. [112] Tata Communications owns five cable landing stations, Reliance Jio owns two, and Bharti Airtel owns three. The state-run telecom operator BSNL owns three landing stations, and Vodafone, Sify, and Global Cloud Exchange own one each.

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. [113] The DoT, under the Ministry of Communications, manages the overall development of the telecommunications sector, licenses internet and mobile service providers, and manages spectrum allocation. [114]

Internet protocol (IP) addresses are regulated by the Indian Registry for Internet Names and Numbers (IRINN). [115] Since 2005, the registry has functioned as an autonomous body within the nonprofit National Internet Exchange of India (NIXI). [116]

The Telecom Regulatory Authority of India (TRAI) was created in 1997 to regulate the telecommunications, broadcast, and cable television sectors. [117] The TRAI Act

mandates transparency in the exercise of its operations, which includes monitoring licensing terms, compliance, and service quality. [118] Its reports are published online, usually preceded by a multistakeholder consultation. [119] An amendment to the TRAI Act in 2000 established a three-member Telecommunications Dispute Settlement and Appellate Tribunal. [120]

There have been some reservations about TRAI's independence in the past. [121] The central government makes appointment and salary decisions for its members. [122] The TRAI Act initially barred members who had previously held central or state government office, but 2014 amendments allowed them to join the regulator two years after resigning from office, or earlier with government permission. [123]

TRAI opinions, however, are generally perceived as free of official influence. [124] For example, in September 2020, TRAI recommended the creation of a multistakeholder advisory body to handle complaints and guidelines on net neutrality. [125]

MeitY has engaged in public consultations around proposed policy and legislative initiatives such as the Personal Data Protection Bill [126] and the policy around National Open Digital Ecosystems (NODE). [127] MeitY also conducted two rounds of consultations on a 2018 draft of the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018. [128] Although MeitY adopted a number of changes suggested by various stakeholders during the consultations, regulations around digital news media and over-the-top (OTT) service providers in the 2021 Intermediary Rules were incorporated without public consultation (see B3, B6, C4, and C6). [129]

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 has been blocked by court or government orders in India. Since such orders, particularly government orders, are not often made public, it is difficult to assess the extent of the blocking. However, government numbers show

an increasing number of requests. In March 2020, MeitY counted the number of blocked websites in 2019 at 3,635, [130] a significant increase from the 633, 1,385, and 2,799 in 2016, 2017, and 2018, respectively. [131] In February 2021, the government revealed that it had issued directions to ban 16,283 websites between 2018 and 2020, including 9,849 websites in 2020. [132] The content said to have been blocked includes websites allegedly seeking to stoke anti-India sentiment, and to damage public order, the security of the state, and the interest and defense of India's sovereignty and integrity. [133] Social media and communication platforms have also been blocked in India, with over 100 mobile apps owned by China-based companies, including TikTok and WeChat, restricted during the coverage period (see A3).

In July 2020, websites of three environment advocacy groups – Let India Breath, FridaysForFuture, and There Is No Earth B—critiquing the draft Environmental Impact Assessment Notification 2020 were blocked for several days. [134] FridaysForFuture's website was blocked after Union Environment Minister Prakash Javadekar filed a complaint under Section 66 of the IT Act stating the group spammed him with emails, which was against the law. [135] MeitY also ordered the blocking of 40 websites, under Section 69A of the IT Act, linked with Sikh for Justice (SfJ), a secessionist group which has been declared as an unlawful operation under the Unlawful Activities Prevention Act. [136] MeitY further blocked another 12 websites associated with SfJ in November 2020 under Section 69A of the IT Act. [137]

A number of users reported difficulty in accessing popular websites and platforms during the coverage period. DuckDuckGo, a privacy-focused search engine, was reportedly blocked by ISPs such as Airtel and Jio for several days in July 2020, following the ban on 59 Chinese-based apps (see A3). [138]

Websites carrying pornographic content and file-sharing capabilities have also been blocked. For example, in May 2020, Reuters reported that the DoT ordered ISPs to block the web-based file-sharing website WeTransfer, citing public interest and national security. [139] An initial block on two specific URLs on the site was replaced by an order applying to the entire WeTransfer website. [140]

Several reports have clarified the technology used to block websites in India. Researchers at the Open Observatory of Network Interference and the Centre for Internet & Society in India reported that Airtel and Jio have been using Server Name Indication (SNI)-based filtering, which entails monitoring the unencrypted server

name indication (SNI) that shows which HTTPS sites a user is visiting, to restrict access to websites on government orders. [141] Out of a dataset of 4,379 potentially blocked websites gathered from publicly available sources, Jio blocked 2,951 websites such as PornHub and collegehumor.com using SNI inspection. [142] In April 2018, research by Citizen Lab found that India was using internet-filtering technology from the Canadian-based company Netsweeper. [143] The group identified 1,158 unique URLs that were blocked, including content related to the Rohingya refugee crisis and websites documenting fatal violence against Muslims in Myanmar and India. [144]

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?	**2** / 4

Civil society, news outlets, and tech companies have reported how government actors order social media and other online platforms to remove content, including that which is protected under international human rights standards. The number of takedown orders of content on social media has increased over the previous years from 500, 633, 1,385, 2,799, and 3,635 requests in 2015, 2016, 2017, 2018 and 2019, respectively, to 9,849 requests in 2020. [145] Moreover, the new Intermediary Rules notified in February 2021 have changed the environment for intermediary liability and require large social media companies to further moderate content on their platforms (see B3, B6, C4, and C6).

During the farmers' protests in early 2021, the government initially directed Twitter to block 257 India-based accounts, including the accounts of the journalism magazine Caravan and the farmer's unions coalition Kisan Ekta Morcha, for allegedly provoking violence, threatening public order, or "making fake, intimidatory and provocative tweets." [146] Some of these accounts used the hashtag #ModiPlanningFarmerGenocide. Twitter initially complied but a few hours later restored access to the accounts, citing international free expression standards. [147] MeitY then cited Section 69A of the IT Act in ordering Twitter to block 1,178 accounts; Twitter complied in part, but did not take action against accounts related to news outlets, journalists, activists, or politicians. [148] Twitter was reportedly told that noncompliance may result in action being taken against them under Section 69A(3) of

the IT Act, which includes the possibility of imprisonment of up to seven years for employees or financial penalty. [149] YouTube also removed music videos in support of the protests, reportedly following a demand by the government. [150]

Amid a second wave of COVID-19 in April 2021, the MeitY reportedly ordered Facebook, Instagram, and Twitter to restrict an estimated 100 posts, including those that criticized the government's handling of the pandemic response and shortages of oxygen and hospital beds. [151] Some of the content requested to be blocked came from opposition politicians and public figures. [152] The Home Ministry alleged that these posts were spreading fake news and inciting panic, and thus hampering the government's response to the pandemic. [153] Facebook also reportedly blocked the #ResignModi hashtag for a few hours, but claimed that the move was done accidentally. [154] In May 2021, Reuters reported that MeitY issued a letter to social media companies asking for the removal of content that used the name or implied the existence of an "Indian variant" of COVID-19. [155]

Criminal charges were brought against streaming platforms over political and religious content during the coverage period. In January 2021, multiple criminal complaints were filed against the makers and writers of the Amazon Prime web series "Tandav" for allegedly hurting religious sentiments and social beliefs when depicting Hindu gods and symbols. [156] Amazon officials were also summoned by the Ministry of Information and Broadcasting (MIB) over the complaints made against the series. [157] The show's makers announced that they would delete the controversial scenes in question. [158] Other state officials also lodged criminal complaints against the series's makers. [159] Similarly in September 2020, a member of Parliament alleged that the MIB minister had asked the Alt Balaji web series "Virgin Bhasskar" [160] to remove a scene depicting a sex racket being run in a hostel named after the venerated, historical leader Ahilyabhai Holkar. [161]

After the government banned 59 mobile applications with links to China in June 2020, Google and Apple removed the apps from their respective app stores (see B1). [162] The government reportedly directed all companies that owned the applications to comply, [163] stating that the apps' continued availability and operation on app stores would constitute a legal offense. [164]

An order that led to the global takedown of content remained under appeal as of February 2021. [165] In October 2019 the Delhi High Court ordered Facebook, Google,

YouTube, Twitter, and other unidentified internet intermediaries to remove videos relating to popular religious leader Baba Ramdev and his business over alleged defamation. The far-reaching order required the platforms to remove the content globally if it was uploaded from India, as well as geo block content to make it inaccessible in India. [166]

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. [167] Intermediary guidelines issued in 2021, which have replaced the 2011 Rules, require intermediaries to remove access to certain content within 36 hours of a government or legal order under Section 79 of the IT Act (see B3). [168] 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 take down orders and not on user complaints. The Court had also clarified that unlawful content beyond the ambit of Article 19(2) (restrictions on the right to the freedom of speech and expression) of the Indian Constitution cannot be restricted. [169]

Intermediaries can separately be held liable for infringing the Copyright Act, 1957 [170] under the law and licensing agreements. [171] The *Shreya Singhal* decision has had no impact on the legal framework on intermediary liability for copyright infringement. A 2012 amendment limited the liability for intermediaries such as search engines that link users to material copied illegally, but mandated that they 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. [172] Rules clarifying the amendment in 2013 gave intermediaries power to assess the legitimacy of the notice from the copyright holder and refuse to comply. [173] However, some critics said the language was vague. [174]

In February 2021, the Indian Cyber Crime Coordination Centre, under the Ministry of Home Affairs, launched the Cyber Crime Volunteers Concept. [175] The Program will allow good Samaritans to volunteer and register themselves as unlawful content flaggers and help law enforcement agencies identify, report, and remove illegal content. [176]

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

Restrictions on digital content are opaque, and there are limited avenues for appeal. The new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, or the Intermediary Rules 2021, impose new obligations for social media companies, OTT platforms, and digital news outlets to regulate or otherwise censor content.

In February 2021, the MeitY enacted the Intermediary Rules 2021 (see B6, C4, and C6). [177] Significant social media intermediaries—defined as companies with at least five million users—have 36 hours from being notified to remove content that is unlawful, including that which undermines the sovereignty of the state, friendly relationships with other states, security, public order, decency, or morality. Content that shows nudity or is a depiction of a sexual act must also be removed within 24 hours of receiving a complaint. 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. The companies must also notify users when their content is removed, provide a clear justification for the decision, and offer an avenue for appeal.

Significant social media intermediaries must appoint three India-based officers. A nodal person of contact is required to coordinate with law enforcement around the clock, while the 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 the Indian Penal Code. [178] In May 2021, MeitY asked significant social media intermediaries to furnish the names and contact details of their three in-country officers. [179]

Separately, social media intermediaries, regardless of their size, must create grievance redressal mechanisms. A grievance officer must acknowledge complaints about content from any user within 24 hours and resolve them within 15 days. [180] The officer is also responsible for orders issued by competent authorities, courts, or other government agencies.

Additionally, the rules subject digital news media and OTT platforms to a regulation system and a Code of Ethics. [181] The code notes that content creators should consider whether content affects India's sovereignty, jeopardizes security, or affects

friendly relations with foreign countries. [182] Further, OTT platforms are cautioned to consider India's multireligious and multiracial society and be mindful of content that relates to religion and race. [183] To enforce the code, a self-regulation body and interdepartmental committee are granted a range of powers, from requesting an apology or disclaimer, to recommending that the government block content under Section 69A of the IT Act 2000.

Exactly how the rules will be implemented remained ambiguous at the end of the coverage period. For example, it is unclear which entities are covered: the rules' definition of digital news platforms is broad enough to cover any actor that publishes noteworthy content about events of a sociopolitical, economic, or cultural nature over the internet, [184] raising questions about whether blogs or niche-content websites will be implicated.

Civil society groups, industry experts, and tech companies have broadly criticized the rules for the increased power they provide the government and their impact on free expression, privacy, and access to information. [185] Several legal challenges questioning their constitutionality and other concerns were underway at the end of the coverage period (see C4). [186] For example, the High Court of Kerala granted interim relief to the online legal news publication Live Law from coercive action by the state under the rules. [187] The Delhi High Court also heard a case brought by the Foundation for Independent Journalism that challenges whether the rules can apply to digital media entities.

Prior to the rules' enactment, other efforts to regulate OTT platforms continued during the coverage period. [188] In September 2020, the Internet and Mobile Association of India (IAMAI) released its third draft of a code for self-regulation with 15 signatories, including Netflix, Amazon Prime, and Disney Plus Hotstar. [189] However, the MIB did not support the draft, citing the lack of monitoring by an independent third party and absence of a well-defined code of ethics, among other things. [190] In February 2021, 17 OTT streaming platforms announced the adoption of a "tool kit" outlining implementation of the September 2020 draft, while including and incorporating the objections of the MIB. [191]

Blocking of websites takes place under Section 69A of the IT Act and the 2009 Blocking Rules, [192] 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." [193] Intermediaries' failure to comply is punishable with fines and prison terms of up to seven years. [194]

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. [195] These requests are reviewed by a committee that includes senior representatives of the law, home affairs, and information ministries, and the nodal agency for cybersecurity, the Indian Computer Emergency Response Team (CERT-In). [196] On receiving the request, reasonable efforts must be made to identify and notify the person or intermediary who is hosting the content in question, and they must be given the opportunity to defend themselves within 48 hours of receiving the notice. [197] The officer chairing the committee issues the approved orders to service providers. In emergencies, the secretary of the MeitY may issue blocking orders directly through written instruction from the designated officer and the emergency order must be placed before the committee for reviewing requests and consideration within 48 hours. [198] Following the recommendation of the committee the secretary of the Department of Internet Technology will pass the final order; if such request is denied, the interim blocking order is revoked and content is unblocked. In January 2020, the Centre for Internet and Society found inconsistencies in ISPs' compliance with the blocking framework established by the IT Act and the Shreya Singhal judgment, with websites blocked by ISPs varying widely. [199]

Indian courts can independently order content takedowns. The designated officer is required to implement the court order after submitting it to the secretary of the MeitY. [200] The Blocking Rules require all content takedown orders issued by the government to remain "strictly confidential." [201] In the landmark 2015 Shreya Singhal case, the petitioners challenged the constitutionality of Section 69A, citing opaque procedures, among other issues. [202] The Supreme Court upheld Section 69A and the Blocking Rules, [203] saying safeguards were adequate, narrowly constructed, and constitutional. [204] However, the court read the Blocking Rules to include both the right to be heard and the right to appeal. Blocking orders must now provide a written explanation, allowing them to be challenged by writ petition, and allow for reasonable efforts to contact the originator of the content for a predecisional hearing. [205]

However, the rules continue to require that the orders and actions based on them be kept confidential; [206] hence there is no information on the extent of compliance with the judgment.

In September 2018, the MeitY ordered the blocking of DowryCalculator.com, a website using satire to criticize the practice of dowry. [207] The owner of the website was reportedly not provided with a hearing or the right to appeal, in contravention of Shreya Singhal. [208] However, in December 2019, a division bench of the Delhi High Court issued a notice to the DoT, the MeitY, and the Ministry of Women and Child Development, in a petition challenging the blocking of the website without complying with the mandated safeguards. [209] As of May 2021, the case was pending before the Delhi High Court.

Judges sought to improve the framework for blocking content under copyright injunctions in 2016, but broad restrictions continued to be observed. 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. [210] In April 2019, the Delhi High Court again allowed copyright holders to seek dynamic injunctions (injunctions against unidentified intermediaries). [211] ISPs have occasionally implemented such orders by blocking entire websites instead of individual URLs, irrespective of whether the websites were hosting pirated material. [212] The judiciary has noted that John Doe orders can lead to excessive blocking, [213] and civil society has called for greater transparency. [214]

In August 2019, the Delhi High Court, while directing ISPs to block several piracy websites (see B1), granted dynamic injunctions allowing the plaintiffs in the case to request that ISPs block, mirror, or redirect websites from the originally blocked sites without further judicial orders. [215] In July 2020, the Delhi High Court again granted a dynamic injunction ordering ISPs to block 118 websites hosting content infringing Disney's copyright, as well as granted Disney the option to add "other rogue websites" if they host similar content. [216] The Delhi High Court extended the use of dynamic injunctions from copyright infringement to cases of trademark infringement in August 2020. [217]

The IT Act and the Indian Penal Code, 1860 (IPC) prohibit the production and transmission of "obscene material," [218] but there is no specific law against viewing pornography in India. The Delhi High Court issued guidelines for intermediaries in

cases of nonconsensual uploading of an individual's pictures onto pornographic websites, and ordered intermediaries and search engines to remove the content immediately and de-index and de-reference it globally. [219] Intermediaries were directed to proactively monitor their websites using automated tools in order to remove content which was "exactly identical" to the offending content mentioned in the court order. [220] Separately, in *Kamlesh Vaswani v. Union of India*, the petitioner asked the Supreme Court to direct the government to block all online pornography. [221] The government informed the Supreme Court that blocking pornography entirely was unfeasible and unconstitutional. [222] The case remained pending as of May 2021.

A 2016 interim order by the Supreme Court had implications for content removal by private companies. The court ordered search engines operated by Google, Microsoft, and Yahoo to "autoblock" advertisements offering services to determine the sex of a child before birth; [223] such advertisements contravene a 1994 law attempting to stop female feticide. [224] The ruling asked search engines to block results for specific search terms and ordering the creation of a nodal agency to oversee the process. [225] Critics feared the ruling would restrict related information and that autoblocking would breach the Shreya Singhal judgment wherein the court ruled that intermediaries were required to take down content only on receipt of a legal demand from the government or a court order. [226]

In November 2020, the High Court of Orissa noted the need for an explicit right to be forgotten, particularly for sexually explicit content. [227] In October, a writ petition to the Kerala High Court cited the right to be forgotten in a request to delete a court order online. The defendant cited a 2017 Supreme Court judgement recognizing the right to privacy as justification for the right to be forgotten. [228]

Social media platforms' removal of content has also lacked transparency and consistency. For example, Caravan's executive editor noted that Twitter did not inform them when it temporarily restricted their account in connection to their protest-related tweets (see B2). [229] Twitter subsequently sent an email stating that the account had been restricted in pursuance of a "legal demand." [230] The Facebook Oversight Board overturned Facebook's decision to remove a video reportedly featuring a social activist stating that the Rashtriya Swayamsevak Sangh (RSS) and the BJP were planning a genocide of the Sikh community, [231] with the board saying that the removal was inconsistent with human rights standards. Facebook had originally

removed the video under Facebook's Dangerous Individuals and Organizations Community Standard.

In August 2020, the *Wall Street Journal* reported that a Facebook executive in India opposed applying the platforms' content-moderation rules to at least one member of the BJP and several other individuals and groups. [232] The employee reportedly told other employees that Facebook's business interests may be hurt if it moderated the content of members of the ruling party. Facebook denied claims of bias and stated that the application of their policies was open, transparent, and nonpartisan. [233] In April 2021, the *Guardian* reported that Facebook failed to remove a network of fake accounts purportedly created to increase the BJP's popularity. [234]

B4 0-4 pts

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

Over the past eight years, threats of criminal charges, the growing influence of the ruling BJP, and increased online harassment have reportedly contributed to more self-censorship among individual people and news outlets. [235] Civil society groups have expressed concern that the Intermediary Rules 2021 may also lead to self-censorship by digital media and OTT platforms (see B3, B6, C4, and C6). [236] Self-censorship over Jammu and Kashmir and COVID-19 in particular has been reportedly common in recent years. [237] Caravan Magazine reported that the central government had repeatedly signaled to the media to refrain from publishing negative views on COVID-19, especially the government's response to the pandemic. [238]

However, many independent online outlets, individual journalists, and ordinary users, including those belonging to marginalized communities, continue to report on and speak publicly about controversial or political topics. [239]

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?	**2** / 4

Manipulated content, disinformation, and misinformation from domestic actors, including political parties and leaders, continued to be present in the online environment in India.

Several reports in recent years have discussed the connection between manipulated content online and the country's political parties. A report from the Oxford Internet Institute (OII) released in September 2019 identified India as having coordinated cyber troop teams linked to both major political parties that manipulate information on Facebook, Twitter, and WhatsApp to amplify their messaging, attack the opposition, and create division. [240] A 2021 OII report also noted that India hosts both paid commentators and volunteers who are coordinated by the state as well as volunteer-run. [241]

An anonymous coder's report published in December 2019 reported that although both the BJP and Congress engage in coordinated activity on Twitter, the BJP's efforts were more sophisticated and more frequent, with nearly 18,000 accounts acting as "seeds" seeking to hijack Twitter trends, compared to only 147 linked to Congress. [242] Reports noted that the BJP seed accounts—which were often followed by ministers but were also decentralized, meaning that removal of individual accounts did not affect the other plants—appeared to generate more abusive content than the Congress ones. [243] The structure followed by Congress, in contrast, was reportedly highly centralized, and did not appear to be associated with ministers or Congress leaders.

In February 2021, Newslaundry published a report detailing how the "Hindu Ecosystem" group, created by a member of the BJP, spread pro-BJP content on social media. [244] The report discusses how a network of over 20,000 participants is given content to spread on Twitter at pre-decided times in order to artificially cause certain hashtags to trend. For example, one group admin reportedly requested members to post against the Tandav television show on Twitter using the hashtag #BanTandavNow, which later trended (see B2). [245]

Disinformation spread online during the farmers' protests; farmers responded by creating an "IT Cell" to combat the campaigns. [246] For example, senior political figures shared a video of supporters of Pakistan in the United Kingdom during the ICC World Cup on social media, claiming that it depicted farmers with pro-Pakistan slogans. [247] Twitter also flagged a video as "significantly and deceptively altered" that

was shared by the head of the BJP IT Cell. [248] The post allegedly attempted to deny an instance of police brutality against a protester. [249]

In May 2021, Twitter labelled tweets by BJP leaders as "manipulated media" that claimed Congress had prepared a "tool kit" to undermine the BJP government over its handling of the COVID-19 pandemic. [250] The label means that Twitter concluded that the tool kit shared by the leaders was "significantly and deceptively altered or manipulated" and would likely impact public safety or cause harm. [251] The government reportedly asked Twitter to remove the tags due to "fairness and equity," and stated that the platform's decision raised questions about their credibility. [252] Following the notice, the Delhi Police reportedly visited Twitter's offices to discuss the incident. [253]

In December 2020, the EU Disinfo Lab reported on a 15-year domestic and international disinformation operation supporting Indian interests, spearheaded by the Srivastava Group and amplified by the news organization ANI. [254] To domestic audiences, the campaign reportedly aimed to foster anti-Pakistan and anti-China sentiment, while internationally it attempted to improve the perception of India and provide a façade of institutional support from the EU Parliament and the United Nations toward the country. [255] EU Disinfo Lab found over 750 fake media outlets and over 550 domain names, operating in 95 countries. [256] The Indian Government rejected any involvement in the operation. [257]

In a 2020 report, Reporters Without Borders (RSF) ranked India as medium-to-high risk for political control over online and offline media distribution networks, [258] citing concerns about outlets majority owned or controlled by political officials and factions, or by a politically connected owner. [259]

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 like OTT content providers were previously not required to register or obtain licenses or provide information about their business entities to publish content in India. However, the Intermediary Rules 2021 imposed new obligations on social media services, digital news publishers,

and OTT platforms (see B3, C4, and C6). Digital news platforms and OTT platforms operating in India will have 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. [260] In May 2021, the MIB published a notice stating that the requirement of furnishing information did not amount to prior registration, and is aligned with similar requirements for offline news. [261]

In August 2019, amendments to the Foreign Direct Investment Policy (FDI Policy) imposed a 26 percent cap for foreign investment in digital media companies, defined as companies that upload or stream news and current affairs through digital media. [262] Additionally, in early 2020, the government mandated that digital media companies need to receive preapproval for foreign investment from certain neighboring countries, including China, and also introduced regulatory approvals necessary for transfer of shares of Indian digital media companies. [263]

It remains unclear which digital media companies are covered under the FDI Policy. [264] In October 2020, the Ministry of Commerce and Industry clarified that entities that stream or upload news on websites, apps, or other platforms and those that transmit news to digital media entities or news aggregators are included. [265] Digital media platforms have until October 2021 to comply with the 26 percent FDI cap. [266] In November 2020, HuffPost India, the Indian edition of US-based Huffington Post, announced that it was shutting down operations in India due to the FDI policy. [267]

The Net Neutrality Rules, adopted in July 2018, are considered among the world's strongest. [268] The rules, with only some exceptions, prevent internet providers from interfering with content, including by prohibiting blocking, throttling, and zero-rating. [269] In September 2020, TRAI recommended that the DoT establish a multistakeholder body to monitor ISPs' compliance with the rules. [270] Providers will have to submit reports to and seek approval from a multistakeholder body about their traffic management practices and any effect on services provided. [271] The body will also work to harmonize and review traffic-management practices, and issue recommendations.

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. The internet has given greater voice to people in remote areas, helping them become part of the national public discourse.

Lack of online content in local languages continues to be an issue (see A2). However, the reporting period has seen a marked increase in consumption and distribution of local-language content. [272] At least one estimate claimed that 70 percent of Indian users could access online news in their local language at the end of 2020. [273]

There remains a lack of representation of minority caste communities in online content and within the broader media environment. [274] An August 2019 report by Oxfam India stated that even when caste-related issues were covered in the news, the majority of those writing on the issues in Hindi and English newspapers were authors from upper-caste communities [275] rather than people from scheduled caste, scheduled tribe, or other backward class communities. [276]

Online spaces for the LGBT+ community have been growing, creating an opportunity for discussing experiences and providing community support. [277] However, civil society groups say LGBT+ people and experiences are still not proportionately covered online, particularly during the pandemic. [278]

Misinformation undermines users' ability to access reliable information. [279] False and misleading information about the COVID-19 pandemic has been rampant on social media platforms, especially WhatsApp. [280] Unreliable information regarding the death toll of Chinese soldiers also spread online amid the India-China border dispute in June 2020. [281]

Misinformation and doctored videos have led to offline violence, with at least 24 people reportedly killed in apparent connection with online activity or content in 2018 alone. [282] Specifically, rumors of child kidnappings and murder have proliferated across the internet in recent years. [283] WhatsApp has taken action by restricting the number of times a message can be forwarded in the country. [284]

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 is popular and has driven important social debates, and at times has helped usher in policy changes. However, local authorities have increasingly imposed internet shutdowns amid protests.

Amid the farmers protests, the government reportedly ordered multiple internet shutdowns for areas in and around New Delhi in January and February 2021 (see A3). [285] Twitter was also ordered to restrict access to several accounts of individuals and organizations sharing information about the protests for Indian-based users (see B2). [286] Local police reportedly monitored social media platforms for accounts spreading purported misinformation and "incendiary" content amid the mobilization, [287] and several journalists and users, including member of parliament Shashi Tharoor, [288] faced legal action for their protest-related online posts (see C3). [289] Despite the increased censorship and other attempts to limit mobilization, social media and other digital platforms were used extensively to disseminate information about opposition to the agricultural laws and live updates on the protests, and to spur national and international conversation. [290]

Additional internet shutdowns were imposed around smaller protests and political mobilization during the coverage period. In October and November 2020, internet services were temporarily suspended in parts of Rajasthan amid protests by the Gujjar community demanding reservations in jobs and education. [291]

Online campaigns continued during the COVID-19 pandemic. As the Indian healthcare system was overwhelmed amid a second wave in April 2021, people turned to social media for organizing relief. [292] Separately, Dalit Human Rights Defenders Network (DHRDNet) and Public Bolti started the #LockdownCasteAtrocities to raise awareness about ways the COVID-19 lockdown aggravated the human rights abuses and discrimination faced by Dalit communities. [293]

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 the internet, and are they enforced by a judiciary that lacks independence?	**4** / 6

The Constitution of India grants citizens the fundamental right to freedom of speech and expression, [294] including the right to gather information and exchange thoughts within and outside India. [295] The right to access information is also recognized as an inalienable component of free expression rights, [296] and press freedom has been read into the freedom of speech and expression. [297] However, these freedoms are subject to certain restrictions in the interests of state security, friendly relations with foreign states, public order, decency and morality, contempt of court, defamation, incitement to an offense, and the sovereignty and integrity of India. These restrictions may only be imposed under a law, and not by executive action. [298]

The judiciary is independent and has played a key role in upholding constitutional rights. However, commentators have observed that the courts may have shown signs of politicization. [299] Despite these assertions, judgments continue to protect free expression. 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, and had led to several arrests for social media posts from 2012 through early 2015. The court in the Shreya Singhal judgment [300] affirmed that freedom of speech online is equal to freedom of speech offline, and held that Section 66A went beyond the reasonable restrictions on freedom of speech specified in Article 19(2) of the Constitution. [301]

In recent years, courts have addressed whether there is a legal recognition of 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 internet and internet infrastructure. [302]

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

The Indian Penal Code (IPC) criminalizes several kinds of speech, that also applies to online content. Individuals can be sentenced to between two and seven years in prison for speech that is found to be seditious, [303] obscene, [304] defamatory, [305] to promote "enmity between different groups on ground of religion, race, place of birth, residence, language," [306] is deemed "prejudicial to maintenance of harmony," [307] or

consists of statements, rumors, or reports that may cause fear or alarm, disturb public tranquility, or promote enmity or ill will. [308] A 2016 Supreme Court judgment upheld laws criminalizing defamation (Sections 499 and 500 of the IPC and Section 119 of the CrPC) as consistent with the Indian constitution. [309]

Internet users are also subject to criminal punishment under the Official Secrets Act for communication of information that may have an adverse effect on the sovereignty and integrity of India. [310] The National Security Act also allows the police to detain an accused person for up to one year without any charge, and has been reportedly invoked against people accused of violations in their speech online. [311]

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. The Supreme Court in 2015 struck down Section 66A, which criminalized speech that, among other things, is grossly offensive or causes annoyance or inconvenience. However, similar complaints continue to be registered under 66A despite the ruling, as well as under Sections 67, 66D, or the IPC (see C3). [312]

State and local government officials have also imposed liability for online speech. In January 2021, an administrative order in Bihar reportedly enabled legal action against users posting offensive, objectionable, or otherwise critical content about state officials on social media. [313] The police later clarified that action would be taken only against posts which "spread rumors and use offensive and defamatory language." [314]

In April 2021, an official in the district of Indore issued an order prohibiting residents from commenting in an "unrestrained manner" on social media about "breaking of corona transmission." [315] The order was narrowed considerably after the Internet Freedom Foundation filed a legal challenge with a district official. [316] Uttar Pradesh's Chief Minister also reportedly directed state officials to charge people under the National Security Act and Gangsters Act for spreading "rumors" about oxygen shortages. [317] In May 2021, the Supreme Court directed state officials and police to not take legal action against people communicating on social media in the hopes of obtaining medical supplies (see C3). [318]

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are	

Users 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.

During the coverage period, journalists and social media users were charged for sedition, promoting enmity between groups, and hurting religious sentiments. [319] Frontier Manipur reporter Kishorechandra Wangkhem was arrested and detained from September to December 2020 on charges of sedition, criminal intimidation, and promoting enmity between groups reportedly over a Facebook comment about a regional government minister's wife. [320] After being granted bail, [321] Wangkhem was again arrested in May 2021 over a Facebook post about the inefficacy of cow dung and cow urine as a cure for COVID-19. [322] Separately, in January 2021, two editors of Frontier Manipur were reportedly arrested and detained overnight on charges of sedition, criminal conspiracy, and supporting a terror organization for criticizing the state's militancy movement in an online article. [323] Another journalist, Prashant Kanojia, was finally granted bail in October 2020 after being reportedly arrested in August over a social media post with an edited image that allegedly defamed a BJP leader (see C7). [324]

In October 2020, Siddique Kappan, a journalist for the news website Azhimukham, was reportedly arrested and initially remanded for 14 days on charges of sedition and violating the Unlawful Activities Prevent Act while he was on his way to cover a murder and sexual assault case (see C7). [325] The Court extended judicial custody, and Kappan was still detained as of June 2021. [326]

Many journalists, activists, and ordinary users were criminally charged and arrested for their online posts amid the farmers' protests. [327] For example, six senior journalists and Congress lawmaker Shashi Tharoor were reportedly charged with sedition, promoting enmity between groups, and criminal conspiracy for claiming on social media that a protestor died in a rally after being shot by police in January. [328] The Supreme Court later stayed the arrests. [329] In February 2021, the Enforcement Directorate, a federal financial investigation agency, reportedly raided the offices of Newsclick.com and several senior staff members. [330] The Editor Guild of India and

civil society groups claimed the raids were intended to harass a news outlet at the forefront of reporting about the protests. [331]

In February 2021, environmental activist Disha Ravi was arrested on charges of sedition and conspiracy in relation to a Google Doc outlining how people can support the farmers' efforts. [332] The police alleged that the "tool kit," which had been shared by climate activist Greta Thunberg on Twitter, was created by Ravi and other activists, and constituted an attempt to cause unrest and defame India. [333] Police also sought data from tech companies related to the case (see C6). Ravi was granted bail after nine days in custody following widespread outrage. [334]

During the country's second wave of COVID-19 in 2021, numerous people were arrested, charged, or threatened with legal sanction in relation to online speech, including content criticizing government authorities (see B2 and C2). For example, in April 2021, one youth was charged under the IPC and the Epidemic Diseases Act for reportedly tweeting a request for an oxygen cylinder for a grandfather who later died. [335] A Facebook user was charged in May 2021 with defamation, criminal intimidation, and intentionally causing harm when criticizing government officials including the prime minister for COVID-19 lockdown policies. [336] Another Facebook user was arrested for reportedly posting "misleading and exaggerated" comments about the prime minister. [337]

During the coverage period, courts themselves penalized users for posts criticizing the judiciary. In August 2020, a two-judge bench of the Supreme Court fined activist and public interest lawyer Prashant Bhushan for tweets criticizing the court, ruling that the posts were not "fair criticism" and amounted to a malicious attack. [338] Civil society organizations have denounced the decision for having a chilling effect on free speech and undermining people's ability to hold state institutions accountable. [339]

Private companies have also pursued legal cases against users for their online activities. In January 2021, journalist Paranjoy Guha Thakurta faced an arrest warrant in a defamation case filed by the Adani Group for an online article claiming that the company benefited financially from adjustments to government rules. [340]

C4 0-4 pts

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

Score Change: The score declined from 3 to 2 due to new requirements under the Intermediary Rules that significant social media intermediaries must be able to identify and disclose the "first originator" of a message if requested by the government or judiciary in certain cases, effectively undermining encryption.

Some restrictions limit anonymity on the internet in India. Prepaid and postpaid mobile customers have their identification verified before connections are activated. [341] There is a legal requirement to submit identification at cybercafés [342] and when subscribing to internet connections.

The Intermediary Rules 2021 impose certain restrictions for anonymity online (see B3, B6, and C6). [343] Significant social media intermediaries, or companies with more than 5 million registered users, must allow users to "voluntarily" verify their accounts using any appropriate mechanism, including using mobile numbers. Companies must clearly mark which users have verified their accounts. While the verification mechanism is "voluntary," digital rights organizations have expressed concerns over the possibility of this being made mandatory in the future. [344]

The government has moved toward weakening encryption, citing the misuse of social media for crime, online sexual exploitation of children, and other public safety concerns. [345] In October 2020, India joined Japan, the United Kingdom, United States, Canada, Australia, and New Zealand in a statement requesting that social media platforms like Facebook and WhatsApp allow law enforcement access to decrypt and provide content in a "readable and usable format." [346]

The Intermediary Rules 2021 require that significant social media 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. [347] Technical experts have raised concerns that such traceability is not possible without breaking end-to-end encryption, [348] despite the government's claim that it did not intend to undermine the technology. [349] In May 2021, WhatsApp filed a suit against the government in the Delhi High Court, arguing that traceability violates the right to privacy. [350]

Earlier, in 2019, the debate over traceability and encryption became intertwined with a petition before the Madras High Court demanding that social media accounts be linked with Aadhaar, the unique identification project that collects and stores biometric and other data including fingerprints, iris scans, and photos of over one billion Indians (see C5). [351] In late 2019, Facebook filed a petition before the Supreme Court requesting that the Madras case be bundled with several petitions before different courts addressing similar issues and heard by the Supreme Court in order to avoid conflicting orders. In January 2020, the Supreme Court approved the request, and ordered the Madras High Court, among others, to transfer all files to the Supreme Court. [352] The case was pending as of May 2021.

ISPs setting up cable landing stations are required to install infrastructure for surveillance and keyword scanning of all traffic passing through each gateway. [353] The ISP license bars internet providers from deploying bulk encryption; restricts the level of encryption for individuals, groups, or organizations to a key length of 40 bits; [354] and mandates prior approval from the DoT or a designated officer to install encryption equipment. [355]

C5 0-6 pts

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

State surveillance of online content and activity, in certain situations, infringes on user privacy. The right to privacy has been protected under several judicial decisions in India. In August 2017, a landmark Supreme Court ruling in the context of Aadhaar recognized privacy as a fundamental right embedded in the right to life and liberty, and intrinsically linked to other fundamental rights like the freedom of expression. [356] In October 2019, the Bombay High Court reiterated the applicability of the right to privacy in the context of wiretapping. [357]

Communications surveillance may be conducted under the Telegraph Act, [358] as well as the IT Act, [359] 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 appears to add another broad category, allowing surveillance for "the investigation of any offence." [360]

The home secretary at the central or state level issues interception orders based on procedural safeguards established by the Supreme Court and rules under the Telegraph Act. [361] These orders are reviewed by a committee of government officials. [362] Interception orders are limited to 60 days, and renewable for up to 180 days. [363] 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. [364] In October 2020, the recording of a phone call between a journalist and the family of deceased victim in a sexual assault case surfaced on social media. [365] It is unclear how the conversation was recorded, and the incident has raised concerns about government phone tapping.

The government's own surveillance equipment is becoming more sophisticated. The Central Monitoring System (CMS), which operates out of Delhi with numerous regional centers, reportedly allows government agencies to intercept any online activities directly, including phone calls, text messages, and VoIP communication, using Lawful Intercept and Monitoring (LIM) systems. [366]

Additionally, NETRA (Network Traffic Analysis), developed by the Defence Research and Development Organization, is surveillance software that can reportedly monitor internet traffic in real time. [367] It has allegedly been in use since 2014 largely for external targets by the Intelligence Bureau and the Research and Analysis Wing, although some domestic agencies under the aegis of the Ministry of Home Affairs may have access to it. [368] The Centre for Internet and Society has reported that there has been little public information about NETRA since 2014; the software's current use remains unclear.

In December 2020, the High Court of the state of Delhi heard a petition from the Centre for Public Interest Litigation and the Software Freedom Law Centre to discontinue CMS, NETRA, and an integrated intelligence grid known as NATGRID. [369] The petition contended that the systems violated users' right to privacy by allowing bulk telecommunications surveillance and data collection. [370] In February 2021, the Ministry of Home Affairs stated that government agencies are not granted "blanket permission" to monitor, intercept, or decrypt information under the three programs, and that oversight is sufficient. [371] The government cited "terrorism, radicalization, cybercrime, [and] drug cartels" in arguing for the need for the systems. [372] The case was pending at the end of the coverage period.

The government is suspected of using sophisticated spyware technology. In October 2019, WhatsApp accused the Israeli company NSO Group of helping governments deploy its spying software Pegasus on the platform and claimed that Pegasus was used to spy on at least two dozen activists, lawyers, academics, and journalists in India in May 2019. [373] While NSO claims to only work with government agencies, the Ministry of Home Affairs, in response to a RTI request, denied that it purchased software from NSO Group. [374] However, when questioned in Parliament about the role of the government in the Pegasus case, the minister of state in the Ministry of Home Affairs did not respond directly, instead referring to Section 69 of the IT Act and Section 5 of the Telegraph Act and saying that "authorized agencies as per due process of law, and subject to safeguards as provided in the rules" can intercept, monitor, or decrypt "any information from any computer resource" in the country. [375] The Internet Freedom Foundation has reported that investigations into the hack remain confidential. [376]

In July 2021, after the coverage period, 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—in a leaked data set. [377] Investigators described the data set as a list of people of interest to NSO Group's clients. While it is unclear how many phones on the list were targeted by Pegasus, investigators found that the spyware infiltrated the devices of at least seven people in India, five of whom are journalists. The Indian government again denied using Pegasus. [378]

Separately, Citizen Lab and Amnesty International reported in June 2020 that they found evidence that at least nine academics, lawyers, writers, and activists were targeted between January and October 2019 with a campaign using spear phishing emails that, if opened, would have installed the spyware NetWire, allowing the sender to monitor communications and other activity. [379] Eight of the targeted human rights defenders were demanding the release of activists arrested in 2018 for allegedly participating in protests and violence in the state of Maharashtra. The other person reportedly targeted was a vocal proponent of the release of a jailed academic with disabilities, GN Saibaba. In February 2021, a report from a US-based digital forensics company was presented to the court in the case. The report found evidence that NetWire was used against Rona Wilson, an accused activist in the case, concluding that documents allegedly found on his laptop were planted. [380]

One activist targeted by both NSO Group and NetWire, Anand Teltumbde, was arrested in April 2020 on charges of instigating violence in public speeches in 2017, [381] and continued to be incarcerated during the reporting period. [382] Amnesty International reports that the case relies heavily on information pulled from the activist's electronic devices. [383]

The government uses Aadhaar for the provision of multiple public services, including food stamps, the Targeted Public Distribution System, and various scholarships and employment schemes. [384] As of August 2020, people can use Aadhaar to authenticate themselves when accessing government services online. [385] The scheme raises key concerns regarding data privacy, security, and usage. [386] Breaches of Aadhaar data were reported in 2017, [387] 2018, [388] 2019, [389] and 2020. [390]

In September 2018, the Supreme Court ruled that Aadhaar is constitutional, but set important limits on the program's use. [391] The ruling held that it was legitimate for the program to be mandatory for government welfare schemes and that Indians must link their Aadhaar number to income tax filings and permanent account numbers. The court also ruled that there were sufficient existing safeguards against security and data breaches. However, Aadhaar numbers cannot be required for services such as obtaining a SIM card, opening a bank account, and receiving educational grants and admissions. In January 2021, the Supreme Court dismissed a batch of review petitions challenging the 2018 decision. [392] In November 2019, the Supreme Court also directed that a seven-judge bench be set up to review the 2018 judgment, which had not formed by the end of the coverage period. [393]

Despite the court's restrictions on Aadhaar, the government promulgated the Aadhaar Ordinance in March 2019. The ordinance allowed for the voluntary use of Aadhaar as proof of identity for bank accounts and mobile SIM connections. [394] In July 2019, the Parliament passed the Aadhaar and Other Laws (Amendment) Bill, [395] a similar law that superseded the March 2019 ordinance. [396] Civil society groups have expressed serious concerns, arguing the law ignores the 2018 Supreme Court ruling. [397] As of May 2021, a case was pending in the Supreme Court that challenged the law. [398]

The draft Personal Data Protection Bill, 2019 has been criticized, particularly in relation to the extensive powers and exemptions it gives the central government (see C6). [399] For example, clause 35 gives state agencies an exemption from complying

with limitations if surveillance is "necessary and expedient" or "in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, [and] public order."

In March 2020, it was reported that the government planned to build a database called the National Social Registry that could track every Indian and reportedly capture a vast amount of personal information including information about individuals' marital status, address changes, financial status, place of employment, number of children, and property owned. [400] The registry will reportedly include data from the Aadhaar database. [401]

There has been a lack of transparency and oversight, and in some cases an insufficient legal framework, to ensure that the use of technology for disease surveillance and enforcement of quarantine measures does not undermine privacy. [402] The contact-tracing app Aarogya Setu was initially made mandatory for large sections of the population. [403] However later, the Union government clarified that no public authority could refuse services to individuals for not having the app; which was upheld by the High Court of Karnataka. [404] The app tracks potential coronavirus exposure and rates each user's risk of infection, using data gleaned from Global Positioning System (GPS) and Bluetooth technology. [405] Government agencies are permitted access to the centralized database that stores the data; [406] the app moreover has poor encryption standards [407] and is amenable to deanonymization.

Social media monitoring is also a concern. In August 2018, the Union Government withdrew its proposal to create a Social Media Communication Hub after the Supreme Court characterized it as a tool of a "surveillance state." [408] However, in August 2020, the government released a similar proposal and invited bids from private entities to monitor online data. [409] Similarly, in May 2020, the publicly operated Broadcast Engineering Consultants India Ltd. released a tender for a project that uses machine learning, link analysis, and other forms of artificial intelligence to monitor social media for disinformation and other false content. [410] The tender requests the establishment of an archive for long-term data retention.

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 data on users, and a variety of government agencies may invoke a range of laws to access the information collected.

Ten separate intelligence bodies are authorized to issue surveillance orders to service providers. [411] Online intermediaries are required by law to "intercept, monitor, or decrypt" or otherwise provide user information to officials. [412] The Telegraph Act levies civil penalties or license revocation for noncompliance, [413] and violations of the IT Act can lead to a maximum ten-year jail term. [414] Unlawful interception is punishable by a lesser sentence of three years. [415]

The Intermediary Rules 2021 changed the way companies must share information with government agencies in certain circumstances (see B3, B6, and C4). The rules require intermediaries to provide the government with data within 72 hours of receipt of a written order for the purposes of identity verification, or for the prevention, detection, investigation, or prosecution of offences under domestic law. [416] The rules also impose new data-retention policies, requiring intermediaries to store information for 180 days. Many civil society organizations have expressed concerns about the lack of transparency and the impact on user privacy. [417] The Supreme Court previously set data retention requirements in September 2018. [418]

The Srikrishna Committee, established in 2017 to create a data protection framework, [419] submitted a draft framework for the Personal Data Protection Bill in July 2018 (see C5). [420] The draft Personal Data Protection Bill, 2019 was subsequently introduced in the lower house of Parliament and referred to a Joint Parliamentary Committee in late 2019. [421] The draft adopts a consent-based model to regulate the collection, processing, and storage of personal data and would establish a Data Protection Authority to oversee compliance. Observers have raised questions about the prospective regulator's independence, transparency, and accountability. [422] The bill also proposes a hybrid data-localization model, raising concerns about surveillance and cybersecurity. [423] The new, more stringent requirements would replace previous Indian policy, which applied a sectoral approach to data transfers and storage in sensitive industries such as telecoms, banking, and healthcare. As of May 2021, the bill remained pending and still under consideration by the joint committee.

Standard Operating Procedures for Lawful Interception and Monitoring of Telecom Service Providers—regulations issued in 2014 [424]—restricted interception to a service provider's "chief nodal officer," and mandated that interception orders be in

writing. [425] Rules issued in 2011 under the IT Act provided for greater protection of personal data handled by companies, [426] but do not apply to the government.

The telecom license agreements require service providers to guarantee the designated security agency or licensor remote access to information for monitoring; [427] ensure that their equipment contains necessary software and hardware for centralized interception and monitoring; and provide the geographic location, such as the nearest Base Transceiver Station, of any subscriber at a given point in time. [428] Under a 2011 Equipment Security Agreement, telecom operators were told to develop the capacity to pinpoint any customer's physical location within 50 meters through a Location Based System (LBS). [429] The agreement remains in effect. [430]

The government also seeks user information from international tech platforms. Following the arrest of environmental activist Disha Ravi, police reportedly asked tech platforms like Zoom, Google, and Facebook to share information related to the tool kit she shared online supporting the farmers' protests (see C3). [431] The police publicly acknowledged Google's cooperation but the company made no comment on the matter.

Between January and June 2020, Twitter reported complying with only one percent of the 2,613 information requests and 6,346 account access requests from the government, making India the second highest requester after the United States. [432] During the same period, the Indian government was also the second highest requester of data to Facebook. [433] The platform reported 35,560 requests for information on 57,295 accounts, with a 50 percent compliance rate. [434] Microsoft reported 642 law enforcement in India requests during the same period. [435]

In January 2021, WhatsApp announced that it planned to update its privacy policy allowing the company to share certain user data with the Facebook network, including Instagram. In February 2021, the Supreme Court issued a notice to WhatsApp raising concern about how these changes would impact Indian users. [436] The Court expressed its intention to intervene and called on the government to do so if the policy was rolled out.

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

Trolling and violent threats for online activity are common. Civil society and media outlets have reported on physical violence during detention and in politically tense circumstances such as protests.

People being held in detention for their online activity have alleged physical violence by authorities. In November 2020, journalist Prashant Kanojia reported that while in detention for 80 days he faced physical violence including electrical shocks, as well as verbal harassment including caste-related slurs (see C3). **437** Journalist Siddique Kappan, who was arrested while covering a story about sexual assault (see C3), reported that while in custody he was beaten, and was denied access to his diabetes medication. **438**

During the farmers' protests, online journalists faced physical violence and abuse. **439** Mandeep Punia, a journalist who worked with the Caravan and the online news portal Junputh, claimed that he and fellow online journalist Dharmender Singh were beaten by police while recording at the protests, and also while in custody. **440**

In March 2021, Newslaundry reported on an online group called Hindu IT Cell, which leverages a network of volunteers to identify, troll, harass, and even report to police people they consider "Hindu-Haters." **441** The report included an example in which the network's members shared a clip of a woman's Instagram video discussing whether the Teej festival was sexist to their Telegram channel of over 3,000 members, leading to the video spreading and the woman being subjected to significant trolling, harassment, and doxing. In another example, a lawyer reported that a mob assembled outside her house in October 2020 after the IT cell circulated her post that included an image raising awareness about sexual assault. **442**

Certain aggressive online commentators routinely abuse their opponents. In September 2020, the Committee to Protect Journalist reported that the anonymous blog Stop Hindu Hate circulated lists of journalists who were allegedly prejudiced against Hindus online, with those on the list fearing for their life. **443** Media reports suggest that much of the trolling appears to align with the BJP's views, although there is limited evidence that government actors are directly involved. **444** Rather, journalists have reported that officials' tacit support of online abuse—indicated by senior leaders following known troll accounts on Twitter **445** and the use of volunteers to post anti-Muslim content across WhatsApp ahead of the 2019 elections

[446]—contribute to a climate in which people who are perceived to oppose popular discourse face intimidation, even as robust political debate continues in many online forums. [447]

However, journalistic reporting have accused BJP officials in some cases to directly disseminate incendiary content or other violent threats online. The *Wall Street Journal* reported in August 2020 that a BJP politician's violent and Islamophobic content on Facebook, including calls for Rohingya Muslims to be shot, violated the company's policies. [448] In February 2021, a YouTube video calling for certain journalists to be executed was reportedly shared widely on Twitter, including by certain leaders of the BJP. [449]

Police and local party workers in states not controlled by the BJP have also harassed dissenting individuals. In September 2020, a navy veteran was reportedly beaten by affiliates of the Shiv Sena party for sharing a cartoon mocking the chief minister of Maharashtra on WhatsApp. [450]

Reports suggest that these forms of abuse and trolling are heightened when the victim is a woman, a member of a minority religion, is from a lower caste, or otherwise identifies within a marginalized group. [451] In April 2020, the hashtag "CoronavirusJihad" began trending on Twitter as false information claiming the Muslim community was spreading the disease circulated widely. [452] A member of parliament and BJP official reportedly shared similar content on Facebook. [453] In May 2020, the government requested Twitter to restrict an old Islamophobic tweet by a BJP member of parliament. [454]

To show support for a jewelry company's advertisement depicting an interfaith marriage between a Hindu woman and a Muslim man, a Muslim woman shared pictures of her own interfaith marriage and received over 40,000 abusive Twitter messages and doxing attempts. [455]

Separately, a May 2021 report detailed a harassment campaign purporting to "auction" Muslim women online, some of whom had reportedly previously criticized the government. [456] The campaign used publicly available social media images and violent sexual language.

Civil society groups have also found that women in politics commonly experience trolling. [457] Amnesty International and Amnesty India's Troll Patrol project found that

women politicians were subject to massive amounts of online trolling, hatred, and misogyny during the 2019 general elections. [458] An Amnesty report stated that one in seven tweets directed at women politicians were abusive in nature, amounting to an average of 113 abusive tweets per day per woman. [459] Women from marginalized communities faced the worst of the abuse: Muslim women faced 94 percent more ethnic and religious slurs, and women from Bahujan backgrounds received 59 percent more abusive caste-based tweets compared to women from privileged upper-caste backgrounds.

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. The Indian Computer Emergency Response Team (CERT-In), which issues periodic advisories about attacks and issues crisis-management plans, [460] reported that there were nearly 1,158,208 cybersecurity incidents in 2020, almost triple the figure from 2019. [461] CERT-In also reported that 17,560, 24,768, and 26,121 Indian websites were hacked during 2018, 2019 and 2020, respectively. [462]

The UK-based Comparitech rated India as the 18th least cyber-secure nation in 2020 out of 76 countries surveyed, an improvement from the country's rank of 15 in 2019. [463] McAfee noted that India was the fifth-most targeted nation in the world. [464] The global security firm Kaspersky observed that an estimated 45 percent of online users in India faced cyberattacks in 2020. [465]

Many cyberattacks are suspected to emanate from actors in China. [466] Hackers reportedly based in China attempted 40,300 cyberattacks across five days in June 2020, amid a border dispute between China and India. [467] The attacks were aimed at hijacking internet protocols, and phishing. [468] In February 2021, the National Critical Infrastructure Protection Centre warned about attempts by a Chinese-based hacking group to break into the Telangana grid control systems. [469]

In October 2020, Mumbai suffered a multihour power outage that took hospitals, transportation, and other critical services down. Government officials and a study by

US-based company Recorded Future first suggested that the attack may have come from China. [470] However, after conducting investigations into the outage, a government minister reported that they found no evidence of Chinese involvement. [471]

Reports suggest that cybersecurity attacks and breaches have increased dramatically since the beginning of the COVID-19 lockdown in March 2020. [472] In June 2020, CERT-In warned about a large-scale phishing campaign in which attackers targeted the personal and financial information of Indian citizens and businesses by impersonating government authorities conveying information regarding COVID-19. [473]

Users in India also experience data breaches. Nearly 110 million users of the payment services app MobiKwik reportedly have had their payment information made available on the dark web, although the company denied the breach. [474] A hacker obtained details of over 1.8 million orders from Domino's Pizza India, including phone numbers, payment details, and credit card information of customers, and put the information in a search engine. [475]

The Information Technology Act is the primary legislation governing cybersecurity, and lays out penalties for damaging computers and computer systems. [476] The IT Act penalizes hacking, introducing malware, and distributed denial-of-service (DDoS) attacks that result in significant damage or disruption to essential services. [477] The law also allows the government to define resources as "critical information infrastructure." [478] In August 2020, Prime Minister Modi announced that the government is developing a new cybersecurity policy to counter increased cyberattacks. [479]

Footnotes

1 Megha Mandavia, "India has second highest number of Internet users after China: Report," The Economic Times, September 26, 2019, https://economictimes.indiatimes.com/tech/internet/india-has-second-hig...; Ajai Sreevatsan, "EmTech 2018: India to account for half of new Internet users in few years: Akamai's Beardsell," Live Mint, March 8, 2018, http://www.livemint.com/Technology/gaxdxNnR3072YkZXICk1JJ/EmTech-2018-I...; Harriet Taylor, "Mary Meeker: India now has more internet users than US," CNBC, June 1, 2016, http://www.cnbc.com/2016/06/01/mary-meeker-india-now-has-more-internet-...; Vlad Savov, "India rises past the US to become the internet's second biggest user," The Verge, June 2,

2016, https://www.theverge.com/2016/6/2/11837898/india-internet-user-populati...; Vyas Mohan, "India Pips US in Number of Internet Users," Huffington Post India, June 2, 2016, http://www.huffingtonpost.in/2016/06/02/india-internet-usage_n_10259450....

2 Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators October – December 2020," April 27, 2021, ii, https://www.trai.gov.in/sites/default/files/QPIR_27042021_0.pdf

3 Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators October – December 2020," ii. https://www.trai.gov.in/sites/default/files/PIR_30062020.pdf

4 Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators October – December 2019," iii. https://www.trai.gov.in/sites/default/files/PIR_30062020.pdf.

5 Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators October – December 2020," xii.

More footnotes

On India

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

See More ›

Country Facts

Global Freedom Score

67 /100 **Partly Free**

Internet Freedom Score

49 /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 2021

Other Years

2020

Be the first to know what's happening.

Join the Freedom House monthly newsletter

Email

Subscribe

ADDRESS

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

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org