# Flygtningenævnets baggrundsmateriale

| | |
|---|---|
| **Bilagsnr.:** | **391** |
| Land: | Indien |
| Kilde: | Freedom House |
| Titel: | Freedom on the Net 2020: India |
| Udgivet: | 2020 |
| Optaget på baggrundsmaterialet: | 16. december 2020 |

Freedom House

# India

FREEDOM ON THE NET 2020

**51**

PARTLY FREE

/100

| | |
|---|---|
| A. Obstacles to Access | 12 /25 |
| B. Limits on Content | 21 /35 |
| C. Violations of User Rights | 18 /40 |

LAST YEAR'S SCORE & STATUS
55 /100 **Partly Free**

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


# Overview

Internet freedom in India declined dramatically for a third straight year. Government authorities increasingly shut off connectivity in a bid to

suppress protests against the Citizenship Amendment Act (CAA), which gives certain non-Muslim groups special access to citizenship. New evidence also pointed to spyware campaigns targeting human rights defenders, adding to an already restrictive environment for privacy. International platforms were increasingly pressured to remove content critical of the government's Hindu nationalist agenda and its actions in Jammu and Kashmir, India's only Muslim-majority state. Meanwhile, both the CAA protests and COVID-19 pandemic led to an information environment plagued by disinformation, often pushed by political leaders themselves. Within this environment, women, religious and marginalized communities in particular experienced online harassment and trolling. In a positive development, the Supreme Court laid down certain safeguards to be followed by the government before ordering internet shutdowns. Both governmental and nongovernmental entities continued their efforts to bridge the country's digital divides.

India maintains a robust electoral democracy with a competitive multiparty system at the federal and state levels, though politics are marred by corruption. The constitution guarantees civil liberties including freedom of expression and freedom of religion, but harassment of journalists, marginalized communities, and other government critics has increased under the current government, led by the Bharatiya Janata Party (BJP).

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

# Key Developments, June 1, 2019 – May 31, 2020

- India continued to be home to more government-imposed internet shutdowns than anywhere else in the world, justified by authorities for reasons including the need to counter disinformation, protests, communal violence, and cheating on exams. Courts directly

responded to the legality of such restrictions during the coverage period (see A3 and C1).

- More political, social, and cultural content was either removed or blocked for India-based users during the coverage period, including information on Twitter about Kashmir and criticism of the government on streaming platforms (see B2).
- In October 2019, the Delhi High Court issued an interim injunction, with worldwide effect, mandating that Facebook, Google, YouTube, Twitter, and other intermediaries remove certain allegedly defamatory videos around the globe if the content was uploaded from India, as well as geolocation block content and render it inaccessible in the country (see B2 and B3).
- In August 2019, amendments to the Foreign Direct Investment Policy imposed a limit of 26 percent on foreign investment in digital media, and required government approval for such investment (see B6).
- The government's harsh response to nationwide protests against the discriminatory Citizenship Amendments Act featured internet shutdowns in at least nine states, including Delhi, as well as arrests for online speech and police violence against online journalists (see B8, C3, and C7).
- Government officials attempted to control the online narrative about the COVID-19 pandemic, issuing restrictions on reporting, arresting and detaining numerous people for their online speech, and reportedly forcing users to remove content from their social media accounts (see B2, B5, C1, and C3).
- Two separate coordinated spyware campaigns were uncovered targeting journalists, activists, lawyers, and other human rights defenders. Activist Anand Teltumbde was targeted by both spyware campaigns and subsequently arrested in April 2020, with the case reportedly relying heavily on information pulled from his electronic devices (see C5).
- Digital monitoring efforts during the COVID-19 pandemic, including the rollout of the closed-source contact-tracing app Aarogya Setu, raised concerns over a lack of transparency, oversight, and other protections for fundamental freedoms (see C5).

# A. Obstacles to Access

*Internet penetration in India continues to improve, with a majority of people going online using their mobile phones. However, inadequate infrastructure still remains an obstacle to access, especially in rural areas. Various governmental and nongovernmental efforts to improve access nationwide are underway. Information and communication technology (ICT) shutdowns ordered by local authorities continued to increase in duration and frequency during the coverage period, positioning the country to be the global leader in connectivity restrictions.*

**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 recorded almost 718.7 million subscribers in December 2019, though only 22.38 million had wired internet connections; approximately 63 percent of users were in urban areas. [2]

While access is expanding, the rate of internet penetration among India's nearly 1.4 billion residents remains low, reaching 54.2 percent in December 2019, [3] though that was up from 46 percent in December 2018. [4] Mobile penetration was much higher, at almost 87 percent by December 2019. [5]

India's average connection speed as of May 2020 was among the lowest in the world, at 11.37 Mbps for mobile internet and at 35.96 Mbps for broadband. [6] In March 2020, India experienced its slowest internet speed since 2018, [7] possibly due to increased strain on networks as the country went into lockdown in response to the COVID-19 pandemic. In the midst of the pandemic, the Cellular Operators Association of India (COAI) requested that the Department of Telecommunications (DoT) direct video streaming services, primarily Netflix, YouTube, Amazon Prime, and Hotstar, to adopt measures to ease pressure on the internet

infrastructure. [8] Subsequently, the major video streaming service providers suspended HD and UHD streaming on cellular networks. [9]

The share of broadband subscribers has significantly increased, from 57.3 percent in September 2016 [10] to 92.1 percent in December 2019. [11] Despite overall growth, India has a relatively low adoption rate for high-speed broadband (faster than 10 Mbps), at just 19 percent as of 2017. [12] The minimum speed required to qualify as broadband in India has been 512 Kbps since 2012, [13] though the Telecom Regulatory Authority of India (TRAI) recommended raising the threshold to 2 Mbps as far back as 2016. [14]

The Economist Intelligence Unit's Inclusive Internet Index 2020 ranks India 68 out of 100 in terms of availability, as determined by quality and breadth of available infrastructure. [15] Similarly, the World Economic Forum's Global Competitiveness Index ranked India 70 out of 141 countries for infrastructure in 2019, [16] down from 63 the previous year. [17] India ranked a low 103 for electricity supply [18] and 120 for ICT adoption, down from 117 in 2018. These rankings suggest that poor infrastructure is still an obstacle to access in India.

A number of ambitious public- and private-sector initiatives to improve access continue. The government is developing free public Wi-Fi zones in major cities. By one count, there were around 300,000 Wi-Fi hotspots in India in mid-2019, [19] with a goal of 10 million by 2022. [20] In 2016, the public-sector company RailTel launched a project, with technical support from Google, to provide free Wi-Fi services at a minimum of 100 railway stations. [21] In February 2020, after making 415 railway stations internet accessible, Google announced its exit from the project; RailTel plans to continue providing free Wi-Fi services at more than 5,600 railway stations. [22] In December 2019, the Delhi Government launched a free Wi-Fi hotspots scheme, [23] with an initial launch of 100 hotspots. The project aims to provide each user with 15 gigabytes of free data per month via 11,000 Wi-Fi hotspots in order to ensure better and wider internet access in the city. [24]

**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 2018 report from the British-based company Cable, India has the cheapest mobile data pricing in the world, with an average cost of $0.26 for one gigabyte of data. [1] According to the Inclusive Internet Index 2020, India slipped eight spots from the previous year and currently ranks 18 out of 100 countries surveyed in the affordability index, defined by cost of access relative to income and the level of competition in the internet marketplace. [2] Similarly, the 2019 Affordability Report released by the Alliance for Affordable Internet ranked India 9 out of 61 low and middle-income countries for affordable and meaningful access, which includes factors like cost, market competition and public access to the internet. [3] The report suggests that although India's position on the access sub-index (measuring broadband availability and the policy environment) is advancing, this movement is offset by the rapidly consolidating market (see A4).

Internet penetration in rural areas is significantly lower than in urban areas, with only 30 internet subscribers per 100 population, compared with 106 per 100 in urban areas. [4] A number of public and private initiatives aim to narrow the urban-rural divide. The government's ongoing Digital India Programme, launched in 2014, [5] aims to extend fiber-optic cables to more rural areas, establish internet-connected common service centers (CSCs), [6] and provide residents with e-literacy programs. [7] The Digital India Programme has also proposed using satellites, balloons, or drones to bring faster digital connections to remote parts of the country. [8]

CSCs continued to provide free internet services in 120,000 locations using a countrywide fiber-optic network under the government-led BharatNet project until March 2020. [9] After March 2020, the government began charging a fee; [10] more broadly, the implementation of BharatNet

has faced delays and uneven progress among states. [11] In July 2020, CSC revealed plans to deploy 5 lakh fibre-to-the-home (FTTH) connections to facilitate high-speed internet in villages by the end of 2020. [12] In December 2019, the government launched another program, the National Broadband Mission, intended to achieve equitable access to internet and broadband services across India, especially in rural areas, via an investment of $100 billion. [13]

Language also remains a barrier to access. With 22 official languages, only about 12 percent of the population of India speaks English, [14] yet a significant proportion of news and other material available to users in India is in English (see B7). [15] Projects to encourage local language usage online are underway. In 2014, the National Internet Exchange of India (NIXI), which operates and manages Indian domain names, launched the Dot Bharat domain for local language URLs. [16] By April 2017, the number of local language users in India had overtaken the number who rely on English. [17] In July 2018, there were 234 million Indian language users online, [18] and with 90 percent of new internet users consuming local language content, [19] this number is expected to grow to 536 million by 2021. [20]

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 [21] finding that only about a third of Indian internet users are women. [22] The divide is particularly stark in rural areas, with women accounting for only 28 percent of internet users. [23] However, the GSMA, a trade body that represents mobile network operators worldwide, noted in its Mobile Gender Gap Report 2020 that the percentage of women who were aware of mobile internet rose from 19 percent in 2017 to 50 percent in 2020. [24] Internet Saathi, a partnership between Google and Tata Trusts to promote digital literacy among rural women, trains hundreds of women per week in villages across the country, [25] and by July 2019 had reached some 70,000 participants. [26]

**A3** 0-6 pts

**2** / 6

| **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?** | |
|---|---|

India is a global leader in the number of internet shutdowns imposed, [1] with shutdowns regulated by broad rules instituted in August 2017. The government does not routinely block the protocols or tools that allow for instant, person-to-person communication.

Local authorities around India have restricted ICT connectivity and usage during times of perceived unrest since at least 2010. [2] 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. [3]

The frequency, geographic distribution, and duration of these shutdowns have increased significantly in the past five years. In 2019, restrictions to connectivity were implemented in at least 16 states at least 121 times, [4] and by July 2020 had occurred in at least 8 states at least 55 times. [5] States and areas affected include parts of Assam, Andhra Pradesh, Madhya Pradesh, Uttar Pradesh, West Bengal, and the National Capital Region (which includes Delhi). [6] Outside the Jammu and Kashmir region, which is excluded from this report's scoring criteria (see Overview), Rajasthan had the highest number of internet shutdowns in 2019, with at least 68 reported incidents. These shutdowns affect both mobile and fixed-line connections, [7] and the majority are short-term restrictions lasting from a few hours up to a week. [8]

During the course of large-scale protests against the controversial and discriminatory Citizenship Amendment Act (CAA) in late 2019 and early 2020, a number of network shutdowns were imposed across the country, including the first such instance in Delhi (see B8). [9] In November 2019, stoppages of internet services were imposed in Uttar Pradesh, Rajasthan and Haryana in anticipation of potential violence after a Supreme Court judgment in the Ayodhya case, a religious dispute that has previously caused large-scale communal violence. [10] The duration of the shutdowns

varied from 24 hours in some parts of Uttar Pradesh to 48 hours in the city of Jaipur in Rajasthan. [11] Similarly, on January 1, 2020, restrictions to mobile and fixed-line internet connections occurred for 15 hours in Koregaon Bhima and neighboring villages in anticipation of potential violence on the anniversary of the Anglo-Maratha Battle of Koregaon. [12] In July 2019, authorities temporarily restricted internet services in 10 towns in Rajasthan's Udaipur district, claiming the need to stop the spread of misinformation after a local man was murdered. [13]

In the Jammu and Kashmir region, which is excluded from this report's scoring criteria (see Overview), the state administration ordered restrictions on internet services on approximately 55 occasions in 2019. [14] Between August 2019 and January 2020, the region, by the orders of the government of Jammu and Kashmir, was subject to 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. [15] Access to 2G networks was restored in the state in January 2020, but 3G and 4G networks remained restricted as of August 2020, [16] except for in two districts of Ganderbal and Udhampur. [17]

Authorities use legal and policy frameworks to order connectivity restrictions, as the government does not exert much control over the internet infrastructure (see C4). Orders to restrict connectivity have usually been justified under Section 144 of the Code of Criminal Procedure, 1973 (CrPC), which permits broad state action to curb any violation of law and order. [18] The Gujarat High Court upheld the use of this general law to order shutdowns in September 2015, [19] and the Supreme Court refused a petition challenging it in early 2016. [20] Section 69A of the Information Technology Act, 2000 (IT Act) permits the central government to order website blocks, while Section 5 of the Indian Telegraph Act, 1885 (Telegraph Act) allows state and central authorities to order that any message not be transmitted in public emergencies, and has been cited in support of service disruptions (see B3). [21]

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. [22] The broad rules authorize only national or state-level officials of a certain rank to issue temporary suspension orders to shut down telecom services in times of public emergency or threats to public safety. These rules mandate that each order should contain reasons for shutdowns of telecom services and should be forwarded to a review committee for assessment. However, several internet shutdown orders imposed since 2017 were issued under Section 144 of the CrPC by officials not designated under the Telegraph Act rules. [23] Civil society groups have raised concerns that some internet shutdown orders were therefore not issued by authorized officials and lacked necessary procedural safeguards and checks. [24]

During the coverage period, courts directly ruled on the legality of connectivity restrictions. The Gauhati High Court ordered the government of the state of Assam to restore mobile internet connectivity eight days after the state administration had indefinitely shut down the internet during CAA protests in December 2019. [25] As of July 2020, another case, involving a 5-day shutdown in May 2020 that affected some districts of West Bengal, remained under challenge at the Calcutta High Court for being issued under Section 144 of the CrPC rather than the 2017 Act rules. [26]

In January 2020, the Supreme Court responded directly to the months-long internet shutdown in Jammu and Kashmir, ruling that the state must review existing shutdown orders in the region, [27] and that connectivity restrictions across the country should be well reasoned, proportionate, temporary, made publicly available, and present the least restrictive alternative (see C1). [28] However, the court did not order the restoration of connectivity in Jammu and Kashmir in full, and critics argued that the ruling failed to address the fundamental question of deprivation of essential access to internet services. [29] A related decision in May [30] reiterated the mandate that a special committee comprised of state and central government officials review the orders, [31] but a suit filed with the court in June alleged that the government had failed to implement the ruling. [32]

**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 2019, there were 358 operational ISPs in India, [1] up from 326 in 2018. [2] While there is no legal monopoly, Reliance Jio has almost 52 percent of the market, and the top three ISPs together control nearly 95 percent of the market. [3] There are seven mobile operators, [4] with Reliance Jio controlling nearly 32 percent of the market and the top three operators controlling over 88 percent of the market. [5] In April 2020, Facebook invested $5.7 billion in a 9.9 percent stake in Reliance Jio, raising concerns regarding potential anticompetitive practices. [6] 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, pending regulatory approval. [7]

A universal license framework, for which guidelines were published in November 2014, [8] reduced legal and regulatory obstacles by combining mobile phone and ISP licenses. Licensees pay a high one-time entry fee, a performance bank guarantee, [9] and annual license fees adjusted for revenue. [10]

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 has been 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. [11] As a result, the cost of operation for telecom service providers will rise considerably. [12] While the court has rejected petitions from telecom operators requesting a review of the order, [13] as of July 2020 it was considering requests to allow operators to pay the fees over 15 to 20 years. [14] 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. [15]

In 2017, the Cybercafé Association of India said that over 70 percent of cybercafés had closed over the previous year. [16] In 2011, the Indian government introduced rules under Section 79 of the IT Act that imposed multiple licensing and monitoring requirements on cybercafés. [17] Critics said the rules were "poorly framed" [18] amid unclear noncompliance penalties and patchy enforcement. CSCs are exempt and operate under separate guidelines. [19]

Roughly 15 submarine cables connect India to the global internet, [20] most of which are consortium-owned. [21] There are at least 15 landing stations where the cables meet the mainland, spread across 5 cities. [22] Tata Communications owns five cable landing stations, Reliance Jio owns two, Bharti Airtel owns three, the state-run telecom operator BSNL owns three landing stations, with Vodafone, Sify, and Global Cloud Exchange owning one each. [23]

**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 Ministry of Electronics and Information Technology (MeitY) formulates policy relating to information technology, electronics, and the internet. [1] 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. [2]

Internet protocol (IP) addresses are regulated by the Indian Registry for Internet Names and Numbers (IRINN). [3] Since 2005, the registry has functioned as an autonomous body within the nonprofit National Internet Exchange of India (NIXI). [4]

The TRAI was created in 1997 to regulate the telecommunications, broadcast, and cable television sectors. [5] The Telecom Regulatory Authority of India Act (TRAI Act) mandates transparency in the exercise of its operations, which includes monitoring licensing terms, compliance, and service quality. [6] Its reports are published online, usually preceded by a

multi-stakeholder consultation. [7] An amendment to the TRAI Act in 2000 established a three-member Telecommunications Dispute Settlement and Appellate Tribunal chaired by a former senior judge. [8]

There are some reservations about the TRAI's independence. [9] Appointment and salary decisions for members remain in the hands of the central government. 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.

TRAI opinions, however, are generally perceived as free of official influence. [10] In January 2020, the TRAI released a consultation paper on "Traffic Management Practices (TMPs) and Multi-Stakeholder Body for Net Neutrality" [11] and sought comments from the public on the rules and composition of a multi-stakeholder governing body for net neutrality. [12] It was also involved in framing net neutrality regulations in 2016, [13] has recommended a reduction in charges levied for use of cable landing stations, [14] and has pitched for lower taxes on telecom services. [15]

# B. Limits on Content

*Blocks of websites and the forcible removal of content continued to affect political and social information during the coverage period. While the digital media landscape remained lively, disinformation and manipulated content plagued the online environment, notably during tense moments such as elections and protests. In a troubling development, local authorities escalated suspensions of internet access during protests, undermining people's ability to use digital tools to mobilize around important issues.*

**B1** 0-6 pts

| | |
|---|---|
| **Does the state block or filter, or compel service providers to block or filter, internet content?** | **3** / 6 |

Political and social information has been blocked by court or government orders in India. Since such orders are not often made public, it is difficult to assess the extent of the blocking. In its 2017 response to a Right to Information (RTI) request, the MeitY confirmed that as many as 23,030 websites or URLs had been blocked. [1] In another acknowledgement that reflects the scale of government blocking, the DoT confirmed in August 2018 that it had requested that 11,045 websites, webpages, and URLs be blocked since 2016. [2] The content said to have been blocked includes social media networking groups and websites allegedly seeking to stoke anti-India sentiment and damage public order, the security of the state, and the interest and defense of India's sovereignty and integrity. [3]

Authorities provided conflicting information about the number of websites newly blocked over the coverage period. In response to an RTI request from the civil society group SFLC.in, the MeitY claimed to have blocked only 20 websites in 2019, but refused to identify them, citing the need to maintain "strict confidentiality" under Rule 16 of the Information and Technology (Procedure and Safeguards for Blocking for Access to Information to Public) Rules, 2009 (or simply, the Blocking Rules). [4] However, in November 2019, in response to a question in the lower house of Parliament, the minister for electronics and information technology revealed that 3,433 websites had been blocked as of October 2019. [5] In March 2020, the MeitY pegged the number of blocked websites in 2019 at 3,635, [6] a significant increase from the 633, 1,385, and 2,799 in 2016, 2017, and 2018, respectively. [7]

In May 2020, the DoT ordered ISPs to block the web-based file-sharing website WeTransfer, citing public interest and national security. [8] An initial block on two specific URLs on the site was replaced by an order applying to the entire WeTransfer website. [9]

A number of users have reported difficulty in accessing popular websites and platforms. DuckDuckGo, a privacy-focused search engine, was blocked by some ISPs for several days in July 2020. [10] In previous years, other websites users have reported as blocked included Reddit; India's biggest free legal database, Indian Kanoon; the website of Telegram; SoundCloud; and various virtual private networks (VPNs). [11] The

blocking of these websites varied depending upon the ISP and location of the user. [12] There is a lack of clarity on whose orders and under what laws these pages were blocked.

In June 2020, after the reporting period and following military clashes along the Indian-Chinese border, the MeitY banned 59 mobile applications owned by China-based companies or otherwise linked to the country, including the social media and communications platforms TikTok, WeChat, and Helo, citing Section 69A of the IT Act. The ministry also claimed that the apps were detrimental to the sovereignty and integrity, defense, and security of India, as well as public order (see B2). [13] Immediately after the ban, the DoT issued orders to ISPs and telecom companies to block the applications on the banned list. [14] In July, the government banned 47 additional mobile applications that were clones of those banned the previous month. [15]

The Delhi High Court in August 2019 ordered the blocking of websites streaming pirated content, including Trailbreakers, EZTV, Katmovies, and LimeTorrents (see B3). [16] Courts have also ordered the blocking of pornographic content. In compliance with an Uttarakhand High Court ruling, [17] the DoT issued blocking orders in October 2018 for 827 sites hosting pornographic content. [18] In July 2019, the MeitY sent a request to the DoT to enforce compliance by ordering the relevant ISPs to restrict access to pornographic websites. [19] In April 2019, the Madras High Court issued an order to ban TikTok, which has 120 million monthly active users in India, also on grounds of “encouraging pornography” (see B2); [20] the ban was lifted after two weeks. [21]

In April 2018, research by Citizen Lab found that India was using internet-filtering technology from the Canadian-based company Netsweeper. [22] The group identified 1,158 unique URLs blocked, including content related to the Rohingya refugee crisis and websites documenting fatal violence against Muslims in Myanmar and India. [23] Some URLs on Facebook, Twitter, and YouTube dedicated to religious minorities were also blocked, but remained available for those accessing the pages through HTTPS.

Following the January 2020 Supreme Court order responding to the internet shutdown in Kashmir (see A3), [24] which is not assessed in this report (see Overview), the government ordered ISPs to only permit access to 153 white-listed websites within Jammu and Kashmir. [25] To do so, ISPs set up firewalls to permit online content deemed "essential," such as banking services and government websites, while filtering out many social media platforms and news outlets. [26] Access to social media websites was restored in March 2020. [27]

**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?** | **2** / 4 |
|---|---|

*Score Change: The score declined from 3 to 2 due to increased removals of political, social, and cultural content, including Kashmir-specific content on Twitter and government criticism on streaming platforms.*

The legal framework for intermediary liability improved following a landmark Supreme Court decision in 2015. However, the coverage period was characterized by an increase in takedowns of political, social, and allegedly defamatory content, as well as a far-reaching court decision that ordered platforms to remove content globally.

Following the August 2019 revocation of Article 370 of the Indian Constitution, which gave special status to the Jammu and Kashmir region, certain Kashmir-specific content on social media platforms was removed or blocked for India-based users. Citing the spread of "misinformation and rumors to disturb peace and calm," [1] the government issued nine orders to Twitter to block or suspend accounts that shared Jammu and Kashmir-related content. [2] The Committee to Protect Journalists identified 93 Twitter accounts being "withheld," and thus not accessible to India-based users, in September and October 2019. The majority of these accounts mentioned Kashmir in their handle or bio or shared Jammu and Kashmir-related content. [3] The account @Kashmirnarrator, for example, shared a mix of political opinions, links to news articles, and local information. In

August and September 2019, Facebook and Twitter reportedly complied with government takedown requests at record-high rates of 90 percent and more than 60 percent, respectively. [4]

Streaming platforms also removed political content during the coverage period. In February 2020, Hotstar, a platform run by Disney, did not air an episode of "Last Week Tonight with John Oliver" in India that criticized Prime Minister Narendra Modi for his role in escalating persecution of marginalized religious groups, notably Muslims. [5] In November 2019, Amazon Prime India removed an episode of "Madam Secretary" due to its references to Hindu extremism, violence against marginalized communities, and Kashmir. [6] Netflix has also censored content on its platform for India-based audiences. [7]

After the government banned 59 mobile applications with links to China in June 2020, after the coverage period, Google and Apple removed the apps from their respective app stores (see B1). [8] Following reports that some of the banned applications were still accessible in July 2020, [9] the government reportedly directed all companies that owned the applications to comply with its orders, while warning that continued availability and operation of the applications would constitute a legal offense. [10] In September, the MeitY again banned additional apps with links to China. [11]

The reporting period also saw several high-profile defamation suits leading to court-ordered content removals. [12] In October 2019, for instance, the Delhi High Court ordered Facebook, Google, YouTube, Twitter, and other unidentified internet intermediaries to take down videos relating to popular religious leader BabaRamdev and his business due to alleged defamatory content. Although only an interim injunction, the far-reaching order required the platforms to remove the content globally if it was uploaded from India, as well as geolocation block content to make it inaccessible in India. [13] As of July 2020, the order remained under appeal in the same court. [14] In January 2020, the Bombay High Court, in a preliminary injunction, ordered a social media influencer to remove content that it deemed disparaging to a corporation's product, arguing that

users with larger followings have a responsibility to ensure that their content is not misleading or false. [15]

Reports also suggest that officials have pressured internet users to remove content. Indranil Khan, an oncologist in Kolkata, for example, was released following a 16-hour detention in March after he deleted posts from his Twitter account about doctors using raincoats as protective health gear during the COVID-19 pandemic. [16] He also stated that he had to post online that state authorities were "working hard for doctors." [17]

Following the 2015 *Shreya Singhal v. Union of India* ruling—in which the Supreme Court ruled that intermediaries were only obligated to take down content upon receiving an order from a court or government authority—Facebook said it would require more formal notifications to restrict content (see C3). [18] Facebook restricted 841 items from July to December 2019, down from 1,300 total restrictions during the previous six-month period. The restrictions were primarily for hate speech, anti-religious content constituting incitement to violence, extremism, and anti-government and anti-state content. Access was restricted to 358 items in response to private reports of defamation. [19]

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. [20] Intermediary guidelines issued in 2011 under Section 79 of the IT Act required intermediaries to remove access to certain content within 36 hours of a user complaint. [21] The government later clarified this rule. [22] In the *Shreya Singhal* case, the Supreme Court reduced the scope of Section 79 and the intermediary guidelines, and companies are no longer required to act on user complaints. Court and government takedown orders, furthermore, are only legitimate if they fall within the reasonable restrictions provided for under Article 19(2) of the constitution. Unlawful content beyond the ambit of Article 19(2) cannot be restricted. [23]

In December 2018, the MeitY released new draft intermediary guidelines intended to replace the 2011 rules under Section 79 of the IT Act (see C4

and C6). [24] Purportedly intended to curb the spread of disinformation and misinformation, the rules mandate that intermediaries deploy automated tools to proactively identify and remove illegal content, including that which harms "public health or safety." Intermediaries—defined broadly to include ISPs, social media platforms, email providers, and cloud services, among others—would have 24 hours to comply with a government removal order. [25] Civil society groups and internet experts urged the government to withdraw the proposal, noting that it conflicts with the *Shreya Singhal* ruling and would be ineffective at limiting disinformation. [26] The MeitY indicated that it would revise the intermediary guidelines in February 2020; [27] however, the move was delayed in order to make the guidelines compatible with the Personal Data Protection Bill, 2019 (see C6). [28]

Intermediaries can separately be held liable for infringing the Copyright Act 1957 [29] under the law and licensing agreements. [30] The *Shreya Singhal* decision has had no impact on the legal framework on intermediary liability for copyright infringement. A 2012 amendment limited 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. [31] Rules clarifying the amendment in 2013 gave intermediaries power to assess the legitimacy of the notice from the copyright holder and refuse to comply. [32] However, critics said the language was vague. [33]

**B3** 0-4 pts

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

The restrictions on digital content are opaque, and there are limited avenues for appeal.

Blocking of websites takes place under Section 69A of the IT Act and the 2009 Blocking Rules, [1] 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." [2] Intermediaries' failure to comply is punishable with fines and prison terms of up to seven years. [3]

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. [4] 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). [5] The "designated officer," who chairs the committee, issues approved orders to service providers; the committee must also notify the source or intermediary hosting the content, who may respond to defend it within 48 hours. [6] In emergencies, the secretary of the MeitY may issue blocking orders directly under written instruction from the designated officer, but the content must be unblocked if the review committee does not approve them within 48 hours. [7]

Indian courts can order content blocks without government approval. The designated officer is required to implement the court order after submitting it to the secretary of the MeitY. Court orders can be challenged in a higher court, but internet users are not consistently notified of their implementation. [8]

ISPs are not legally required to inform the public of blocks, and the Blocking Rules mandate that executive blocking orders be kept confidential. [9] In the landmark 2015 *Shreya Singhal* case, the petitioners challenged the constitutionality of Section 69A, citing opaque procedures, among other issues. [10] The Supreme Court upheld Section 69A and the Blocking Rules, [11] saying safeguards were adequate, narrowly constructed, and constitutional. [12] 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 pre-decisional hearing. [13] However, the rules continue to require that the orders and actions based on them be kept confidential; [14] it is difficult to know 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. [15] The owner of the website was not provided with a hearing or the right to appeal, in contravention of the safeguards laid down by the Supreme Court in *Shreya Singhal.* [16] 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. [17] As of July 2020, 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. [18] In April 2019, the Delhi High Court again allowed copyright holders to seek dynamic injunctions (injunctions against unidentified intermediaries). [19] ISPs have occasionally implemented such orders by blocking entire websites instead of individual URLs, irrespective of whether the websites were hosting pirated material. [20] The judiciary has noted that John Doe orders can lead to excessive blocking, [21] and activists have called for greater transparency. [22] In August 2019, the Delhi High Court, while directing ISPs to block several piracy websites (see B1), also 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. [23]

In July 2016, a ruling by the Bombay High Court laid down rules for seeking John Doe orders, limiting blocks to URLs, not entire domains, and allowing all affected content to be unblocked after 21 days if a court order

is not obtained. [24] The court also dictated an unambiguous block message and suggested the appointment of an independent ombudsman to oversee implementation. [25] Observers hailed this as a progressive and nuanced approach, [26] but the same month, the Delhi High Court separately ruled that John Doe orders could continue to be used to block websites if more than one page on the site was identified as a potential source of copyright violations. [27]

In October 2019, a single-judge bench at the Delhi High Court issued a global takedown order in a defamation suit (see B2). The injunction was issued against Facebook, YouTube, Google, and Twitter as well as other John Doe internet intermediaries.

The IT Act and the Indian Penal Code, 1860 (IPC) prohibit the production and transmission of "obscene material," [28] but there is no specific law against viewing pornography in India. Child sexual abuse imagery is prohibited under the IT Act (see C2). [29] Extreme child sexual abuse is blocked based on guidance from Interpol, [30] but other restrictions threaten content that has not been found to break the law. In the *Kamlesh Vaswani v. Union of India* case, the petitioner asked the Supreme Court to direct the government to block all online pornography. [31] The government informed the Supreme Court that blocking pornography entirely was infeasible and unconstitutional. [32] The case remained pending as of July 2020, amid additional attempts to block websites carrying pornographic content based on orders issued by different state courts (see B1).

In August 2019, Parliament amended the Protection of Children from Sexual Offences Act 2012 (POCSO Act). The amended law redefined "child pornography" and enhanced penalties for defendants found guilty of a range of acts, including sharing child sexual abuse imagery online. [33]

An2016 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 "auto-block" advertisements offering services to determine the sex of a child before birth, which contravened a 1994 law in an attempt to stop female feticide. The ruling went further than delisting specific content, asking search engines to

block results for specific search terms and ordering the creation of a nodal agency to oversee the process. [34] Critics feared the ruling would restrict related information and breach the *Shreya Singhal* judgment. [35] A subsequent order in April 2017 also directed the search engines to set up an in-house expert body to monitor and block content that would contravene the law; however, this order was reversed in December 2017, with the court reaffirming its previous directions. [36]

Regulations related to content on streaming platforms have been of increasing interest in recent years (see B2). Since May 2019, a petition regarding such regulation has been pending before the Supreme Court. [37] In early 2020, four video-streaming platforms (Hotstar, Voot, Jio, and Sonyliv) signed a Code for Self-Regulation of Online Curated Content Providers, but other widely used streaming platforms did not sign on. [38]

**B4** 0-4 pts

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

While self-censorship is generally not widespread, threats of violence have resulted in people as well as news outlets censoring online content. Over the past six years, threats to press freedom, the growing influence of the ruling BJP, and increased online harassment have contributed to more self-censorship. [1] In December 2017, for example, threats by right-wing trolls prompted the administrator of the political satire Humans of Hindutva to take down its Facebook page; [2] a few months later he declared he would not be intimidated and reactivated the page. [3] The significant political unrest and associated government restrictions during the reporting period, including the revocation of Jammu and Kashmir's special status, the CAA protests, and the COVID-19 pandemic, resulted in a growing perception of self-censorship among the media as well as citizens. [4]

However, many independent online media platforms, individual journalists, and ordinary users, including those belonging to marginalized

communities, continue to report on and speak publicly about controversial political topics.

**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, plague the online environment in India.

A report from the Oxford Internet Institute (OII) released in September 2019 identified India as having coordinated cybertroop teams that manipulate information on Facebook, Twitter, and WhatsApp to amplify their messaging, attack the opposition, and create division. [1] The report found evidence that Indian teams range in size from 50 to 300 people. Both of the leading political parties in India, the BJP and Indian National Congress, have IT cells that have used automation, trolling, and disinformation techniques as a part of political campaigning on social media. [2] Prior to their successful 2014 campaign, BJP politicians were accused of paying citizens and specialized companies to post messages of support and artificially boost their popularity on social media. [3] During the 2019 election period, [4] Amit Malviya, the national head of the BJP information technology unit, was an administrator of a BJP WhatsApp group that described itself as a league of “Hindu warriors working to save nation from break India forces led politically by congress, communist and religiously by Islam and Christianity [sic].” [5]

An anonymous coder’s report published in December 2019 found that although both the BJP and Congress engage in coordinated activity on Twitter, the BJP’s efforts are more sophisticated and more frequent, with nearly 18,000 accounts that act as “seeds” seeking to hijack Twitter trends, compared to only 147 linked to Congress. [6] Reports noted that the BJP seed accounts—which were often linked to ministers but were also decentralized, meaning that removal of individual accounts inflicted

minimal damage on the larger operation—appeared to be generate more abusive content than the Congress ones. The structure followed by Congress, in contrast, was highly centralized, and did not appear to be associated with ministers or Congress leaders. [7]

Disinformation spread rapidly amid nationwide protests against the CAA, including from members of political parties. [8] For instance, unsupported claims by Amit Malviya circulated widely that protesters were paid to participate. [9] In January 2020, a BJP member of parliament claimed online that Hindu families in Malappuram were not given water because they supported the CAA. [10] Earlier, in July 2019, false claims that a local temple in Old Delhi had been vandalized quickly generated nearly 80,000 tweets and were trending on Twitter, with BJP party leaders sharing the associated hashtag as well. [11] Misleading and inflammatory content appears frequently on Prime Minister Narendra Modi's NaMo app, which has been marketed to all Indians as a way to keep up with official government news. [12]

Government officials and state institutions attempted to control the online narrative about the COVID-19 pandemic. Citing the danger of "fake and inaccurate" news, the government in March 2020 unsuccessfully requested that the Supreme Court allow it to exercise prior restraint over coronavirus-related media content. The court did state that the press should ensure coverage of government-issued daily news bulletins (see C1). [13]

The government also focused on curbing coverage that cast India's pandemic response in a negative light, including by limiting journalists' ability to attend health-related press briefings. [14] In several regions including Delhi, government orders barred doctors and healthcare workers in state hospitals, as well as employees of state-owned banks, from posting critical information to social media or communicating with media outlets. [15]

Disinformation and doctored videos have led to offline violence, with at least 35 people killed in apparent connection with online activity or content in 2018 alone. [16] Specifically, rumors of child kidnappings and murder

have proliferated across the internet, such as a video featuring images of corpses—actually showing children killed in Syria—while audio warns Indian parents to be vigilant of kidnappers in the area. [17] In April 2020, three people were killed in the state of Maharashtra [18] after a mob attacked them, reportedly after the spread of rumors across online platforms about thieves and child kidnappers coming into the village. [19] In May 2018, a transgender woman was killed in Hyderabad after a WhatsApp message claimed that transgender women were planning to kidnap children. [20] WhatsApp has taken action by restricting the number of times a message can be forwarded in the country. [21]

The government has actively discussed regulating and monitoring social media. In the lead-up to the 2019 elections, the Election Commission of India (ECI) established a panel to help curb misinformation on Facebook, WhatsApp, and YouTube (see B2). [22] Steps included a Voluntary Code of Ethics that established a communications channel between platforms and ECI officials. The code also aimed to provide more transparency regarding the sources and legitimacy of political advertising, [23] but observers suggested it would be ineffective, in part because development and launch were undertaken too close to the election. [24]

Reporters without Borders ranks India as medium-to-high risk with respect to political affiliations and control over online and offline media distribution networks, [25] citing concerns about media outlets that are majority owned or controlled by political officials and factions, or by a politically-connected owner. [26]

**B6** 0-3 pts

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

*Score Change: The score declined from 3 to 2 due to new limits to foreign investment in digital media outlets and government approval requirements that impose economic and regulatory constraints on the ability to publish content online.*

Online news outlets, blogs, and other publishing platforms are not required to register or obtain licenses. However, in August 2019, the Indian government introduced amendments to the Foreign Direct Investment Policy (FDI Policy) imposing new limits on foreign investment in digital media, which could serve as an economic barrier to publishing for some outlets.

The FDI Policy mandates caps on the percentage of foreign control for Indian companies, and is distinct across sectors. The August 2019 amendments introduced a new cap of 26 percent on foreign investment in digital media companies—defined as companies "Uploading/Streaming of News & Current Affairs through Digital Media"—in comparison to 49 percent and 26 percent caps for television and print media, respectively. [1] Such foreign investment must also be specifically approved by the government. This policy change has been criticized as an effort to enhance control over India's increasingly popular digital outlets, which have sought to raise money from foreign investors due to constraints in the Indian market. [2]

In July 2018, India adopted new net neutrality rules proposed in November 2017 by the TRAI. [3] The rules, with only some exceptions, prevent internet providers from interfering with content, including prohibiting blocking, throttling, and zero-rating. [4] Breaking the rules could result in operators losing their licenses in the country. By some accounts, the new rules make India the strongest backer of net neutrality in the world. [5] In early 2020, the TRAI published a policy document that discussed the governing structure of a multi-stakeholder body to ensure that net neutrality rules are enforced. [6] The TRAI called for comments on the paper and is expected to issue recommendations. [7]

**B7** 0-4 pts

| **Does the online information landscape lack diversity?** | **3** / 4 |
|---|---|

Online media content is diverse and lively. The internet has given voice to people in remote areas, helping them become part of the public

discourse. The Delhi-based company Gram Vaani operates a Mobile Vaani initiative, using an interactive voice response (IVR) system to disseminate reports by mobile phone users to different audiences and stakeholders. It enables over 80,000 households across 12 states to create their own media. [1] However, increased online harassment, disinformation, and disparities in access, among other things, continue to restrict the diversity of the online information landscape.

A lack of content in local languages continues to limit diversity. However, the 2019 general elections resulted in an increase in news reports in local or vernacular language. [2] In May 2020, the first online magazine in Santali was published by Santali-language activists from the state of Odisha. [3]

Issues regarding the lack of online representation of minority caste communities were particularly salient in the reporting period. 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, including in their online versions, were authors from upper-caste communities [4] rather than people from scheduled caste, scheduled tribe, or other backward classes communities. [5]

**B8** 0-6 pts

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

*Score Change: The score declined from 5 to 4 due to government authorities restricting connectivity across the country and other harsh actions taken to quell nationwide protests against the Citizenship Amendments Act.*

Digital activism is popular and has driven important social debates, and at times has helped usher in policy changes. However, while online tools used to mobilize generally remain available in the country, local

authorities have increasingly imposed internet shutdowns to restrict protests.

Online tools were used extensively to organize and raise support for the nationwide protests against the CAA in December 2019, even as government authorities escalated network shutdowns across the country, imposing restrictions in at least nine different states to undermine people's ability to use digital technology (see A3). [1] In one instance, the government ordered service providers to suspend internet services in parts of Delhi for around four hours as protesters were planning to organize at the historic Red Fort.

The government's repression of CAA protests also featured surveillance, arrests and other penalties, and in some cases, violence related to online activity (see C3, C5, and C7). For instance, authorities announced they were monitoring social media for "misinformation," reporting content to social media platforms, and conducting other forms of surveillance. [2] The Union Ministry of Human Resources (which governs higher education) reportedly requested that government-funded universities monitor the social media accounts of teachers and students in order to keep tabs on any involvement in the protests, [3] although the ministry denied the report's authenticity. [4] Separately, the state government of Assam reportedly issued a circular indicating that public officials could face disciplinary action for sharing political opinions online. [5] In Uttar Pradesh, police arrested 124 people in December for allegedly posting content that could incite violence (see C3). [6]

In addition to CAA mobilization, state authorities imposed temporary internet shutdowns in response to other protests and political actions during the coverage period. For instance, in November 2019, internet services were temporarily restricted in four districts in Madhya Pradesh as residents attempted to mark the Islamic holiday Eid-e-Milad-un-Nabi with a procession, despite a local ban on such activity. [7] Similarly, in July 2019, a five-day internet shutdown occurred in the Meerut district of Uttar Pradesh after members of the district's Muslim community organized protests against the killing of a Muslim man accused of theft. [8]

The #MeToo movement has gained substantial online traction across the country, making the conversation on sexual and other forms of gender-based harassment much more mainstream. [9] A range of allegations against prominent men surfaced online after a Bollywood actor shared her sexual harassment story in September 2018.

# C. Violations of User Rights

*Arrests for online activity increased during the coverage period, especially in the context of CAA protests and the COVID-19 pandemic, including political speech that local authorities deemed derogatory or objectionable. The Personal Data Protection Bill introduced in Parliament contains provisions that allow government surveillance, create new criminal liabilities, and establish a data protection agency that was seen as susceptible to politicization; the legislation, which was pending at the end of the coverage period, prompted concern among civil society groups and tech companies. Concerningly, two separate revelations point to coordinated spyware campaigns against human rights defenders.*

**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, [1] including the right to gather information and exchange thoughts within and outside India. [2] Press freedom has been read into the freedom of speech and expression. [3] 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, not by executive action. [4]

A 2015 Supreme Court ruling struck down a problematic provision of Section 66A of the IT Act, which had 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 [5] affirmed that freedom of speech online is equal to freedom of speech offline and held that Section 66A went beyond reasonable restrictions on freedom of speech specified in Article 19(2) of the constitution. [6]

The reporting period also saw some movement toward 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. [7] The court also held that the right to education includes the right to access to the internet, as well as the right to privacy under Article 21 of the constitution. [8]

In January 2020, the Supreme Court examined the legality of internet shutdowns for the first time in the context of the complete shutdown of services in Jammu and Kashmir (see A3). [9] A three-judge bench of the court observed that any internet shutdown order in the country must be well reasoned, proportionate, and present the least restrictive alternative. [10] However, the court did not specifically address the question of whether there is a fundamental right to access to internet services. [11]

During the nationwide lockdown amid the COVID-19 pandemic, a number of attempts were made to limit the reporting of information perceived to be detrimental to the country or the government (see B5). The Supreme Court rejected a gag order or other harsh measures, but suggested that the media is responsible to ensure that all reports are verified, and should rely on government sources of information by including government bulletins in their reporting on the issue. [12]

**C2** 0-4 pts

| **Are there laws that assign criminal penalties or civil liability for online activities?** | **2** / 4 |
|---|---|

The IPC criminalizes several kinds of speech and applies to online content. Individuals can be sentenced to between two and seven years in prison for speech that is found to be seditious, [1] obscene, [2] defamatory, [3] "promoting enmity between different groups on ground of religion, race, place of birth, residence, language," [4] committing acts "prejudicial to maintenance of harmony," [5] or consisting of statements, rumors, or reports that may cause fear, alarm, disturb public tranquility, or promote enmity or ill will. [6] Internet users are also subject to criminal punishment under the Official Secrets Act for wrongful communication of information that may have an adverse effect on the sovereignty and integrity of India. [7]

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). [8]

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. [9] The sections have been used against online speech in the past. [10]

In October 2019, the Andhra Pradesh state government issued an order permitting certain government officials to file defamation suits against journalists. The order was intended to prevent the spreading on electronic and social media of "false, baseless and defamatory news with malafide interest" that can damage the image of government and government officials. [11]

**C3** 0-6 pts

| **Are individuals penalized for online activities?** | **2** / 6 |
|---|---|

Journalists, activists, artists, and members of the public are arrested and detained for political, social, and religious speech or other forms of content authorities deem objectionable or derogatory. Notably, arrests for online activities were frequent during major political events and other crises during the coverage period, including the revocation of Jammu and Kashmir's special status, nationwide protests against the CAA, and the COVID-19 pandemic.

In September 2019, activist Shehla Rashid was charged with sedition for her tweets raising concerns about developments in Kashmir and alleging human rights violations by the Indian Army. [1] In February 2020, poet Siraj Bisaralli and journalist Rajabaxi HV were charged and later released on bail under Section 505 of the penal code after a BJP member filed a complaint with police. [2] The complaint stemmed from Bisaralli's recitation of a poem critical of the CAA and the India National Register in January in Karnataka , video of which was posted to social media by Rajabaxi. In July 2019, police in the state of Assam charged 10 poets for uploading a poem that mentioned allegedly discriminatory practices related to the National Register of Citizens in Assam. The poets were accused of criminal conspiracy, sedition, and inciting disharmony and violence. [3] In December 2019, amid the CAA protests, Uttar Pradesh Police arrested 124 people for allegedly posting objectionable content on social media that "incited" violence. [4]

In April 2020, Zafarul Islam Khan, a journalist who is also the chair of the Delhi Minorities Commission, was charged with sedition and promoting enmity between groups following a complaint alleging that his social media posts referring to discrimination against Muslims in India and the reactions in Middle Eastern countries were causing disharmony and creating a rift in the society. [5] Separately, in November 2019, after the Supreme Court announced the Ayodhya verdict (see A3), authorities arrested around 90 people in Uttar Pradesh and Madhya Pradesh for posting allegedly objectionable content on social media. [6]

In June 2019, police in Uttar Pradesh detained four journalists for posting and sharing a video on social media that allegedly contained objectionable content regarding the Uttar Pradesh chief minister, and

charged them under Section 66A of the IT Act and Sections 500 and 505 of the IPC. [7] Days later, the Supreme Court ordered the immediate release on bail of one of the prominent journalists, Prashant Kanojia; [8] another journalist was granted bail by the Allahabad High Court in July 2019. [9] Kanojia was again charged in April 2020 for allegedly making derogatory remarks on social media against Prime Minister Modi and the chief minister of Uttar Pradesh. [10]

In April 2020, Siddharth Vardarajan, founding editor of the news website Wire, was charged under Sections 188 and 505(2) of the IPC, which sanction charges for disobedience of an order issued by a public servant and promoting enmity or hatred, respectively. [11] The charge stemmed from a Wire article criticizing an event related to the Hindu festival Ram Navmi held during lockdown, in which a sentence of the article wrongly attributed a quote to the chief minister of Uttar Pradesh. [12] Vardarajan had also posted the quote while sharing the article on Twitter. Vardarajan later issued a clarification, and the article was also edited to reflect the correct information. Civil society groups condemned the charges as an attack on press freedom. [13]

During the COVID-19 pandemic, numerous people, including journalists and healthcare workers, were arrested, charged, or threatened with criminal charges in relation to online speech, including content criticizing or questioning government authorities (see B2). [14] At least 55 reporters had been arrested, booked, or threatened for reporting on the pandemic during the lockdown period between March 25 and May 31, 2020, although not all arrests were linked to online activity. [15] In May 2020, journalist Dhaval Patel was arrested and charged with sedition after he claimed in an online article that Gujarat chief minister Vijay Rupani might be replaced for mishandling the COVID-19 crisis in the state. [16] He was granted bail by the Sessions Court after nearly three weeks in detention. In April 2020, freelance journalist Zubair Ahmed was arrested for allegedly spreading false information and obstructing virus containment efforts by the government after he posted a query on Twitter asking why families who had spoken with confirmed patients on the phone were being forced to quarantine; [17] he was later released on bail. Also in April 2020, Andrew Sam Raja Pandian, the founder and chief executive of the news portal

SimpliiCity, was arrested for violating the Epidemic Diseases Act and the penal code after a story accused the government of corruption in food distribution. [18]

People continued to be subjected to criminal penalties for acts of online expression during the coverage period, in many cases for spreading misinformation. [19] In March 2020, police in Kolkata arrested a woman under Section 66C of the IT Act for allegedly spreading false information about a doctor contracting the virus. [20] Similar arrests occurred in Uttar Pradesh, [21] Karnataka, [22] and Mizoram. [23] In Rajasthan, a health worker was arrested for posting false information on social media regarding the number of positive COVID-19 cases. [24]

The National Security Act allows the police to detain an accused person for up to one year without any charge. Between November 2018 and May 2019 journalist Kishorechandra Wangkhem was held in detention after being charged under the Act for social media posts containing vociferous and somewhat incendiary criticism of Manipur state BJP officials and Prime Minister Modi. [25] Wangkhem had already been arrested and charged with sedition under the IPC, but a court later ruled that his critical posts were legitimate expressions of opinion and not seditious, and ordered his release.

Despite the Supreme Court's 2015 decision striking down Section 66A of the IT Act, there were 45 arrests under it between January and September 2018, most likely due to police being unaware of the ruling. [26] For example, one user in Assam was arrested in November 2018, in part under section 66A, for allegedly posting "derogatory" comments about a local government official on social media. [27]

There have been several cases of arrests of people in Jammu and Kashmir, which is excluded from this report's scoring criteria, for their online activity. [28]

**C4** 0-4 pts

| **Does the government place restrictions on anonymous communication or encryption?** | **3** / 4 |
|---|---|

Some restrictions limit anonymity on the internet in India, although users can freely use encrypted technology.

Prepaid and postpaid mobile customers have their identification verified before connections are activated. [1] There is a legal requirement to submit identification at cybercafés [2] and when subscribing to internet connections.

The government has ramped up efforts to work around encryption, citing a number of deaths based on the spread of misinformation through WhatsApp. Proposed in December 2018, draft intermediary guidelines under Section 79 of the IT Act could undermine encryption (see B2 and C6). [3] The rules would require "traceability," which would force intermediaries such as encrypted platforms to provide the originator of content if requested by the government. [4] In order to provide this information, intermediaries may have to break encryption on their platforms. [5]

In June 2019, the government reportedly asked WhatsApp to digitally fingerprint messages sent on the platform in order to trace the sender of a message. [6] Anonymous government officials clarified that requests for such tracing would be limited. [7] In response, WhatsApp maintained its earlier stance that any technological solution to trace the origin of messages would fundamentally compromise end-to-end encryption. [8]

In 2019, the debate over traceability and encryption became intertwined with a petition before the Madras High Court, in the state of Tamil Nadu, demanding that in order to verify users social media accounts should 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). [9] 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. [10] The case was pending as of July 2020.

**C5** 0-6 pts

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

*Score Change: The score declined from 2 to 1 due to two separate coordinated spyware campaigns targeting activists, journalists, lawyers, and other human rights defenders.*

Significant state surveillance of online content and activity infringes on users' right to privacy. Reports during the coverage period uncovered two separate coordinated spyware campaigns against journalists, activists, lawyers, and other human rights defenders.

In October 2019, WhatsApp revealed that its security had been compromised and accused the Israeli company NSO Group of helping governments deploy its spying software Pegasus on the platform. WhatsApp reported that Pegasus was used to spy on at least two dozen activists, lawyers, academics, and journalists in India in May 2019. [1] 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. [2] However, when questioned in Parliament about the role of 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. [3]

Separately, Citizen Lab and Amnesty International revealed in June 2020 that at least nine academics, lawyers, writers, and activists were targeted between January and October 2019 with a campaign using spearphishing emails that, if opened, would have installed the spyware NetWire, allowing the sender to monitor communications and other activity. [4] 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 targeted was a vocal proponent of the release of a jailed academic with disabilities, GN Saibaba.

One activist targeted by both spyware campaigns, Anand Teltumbde, was arrested in April 2020 for allegedly instigating violence in public speeches in 2017. [5] Amnesty International reports that the case relies heavily on information pulled from the activist's electronic devices. [6]

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, liberty, and freedom of expression. [7] In October 2019, the Bombay High Court reiterated the applicability of the right to privacy in the context of wiretapping. [8] The court held that interception orders contested in a bribery case were illegal, and the evidence obtained inadmissible, as the orders were not issued in situations of "public emergency" or "public safety" as required under Section 5(2) of the Telegraph Act. [9]

Communications surveillance may be conducted under the Telegraph Act, [10] as well as the IT Act, [11] 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." [12]

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, [13] which are reviewed by committee of government officials. [14] Interception orders, which are not reviewed by a court, are limited to 60 days, renewable for up to 180 days. [15] 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. [16]

Besides retrieving data from intermediaries, the government's own surveillance equipment is becoming more sophisticated. The Central Monitoring System (CMS) allows government agencies to intercept any online activities directly, including phone calls, text messages, and VoIP

communication, using Lawful Intercept and Monitoring (LIM) systems on intermediary premises. [17] In May 2016, the minister for communications and IT stated that the monitoring centers were already operational in Delhi and Mumbai. [18] More centers were due to be rolled out across the country, but no updates were available in mid-2020.

The government uses Aadhaar enrollment for the provision of multiple public services, including food stamps and cell phone connection. [19] The scheme raises serious concerns regarding data privacy, security, and usage, [20] as well as the relationship between the project and private companies such as Microsoft, Amazon, Facebook, and Google (see C6). [21] In 2017, it was reported that millions of Aadhaar records had been treated as publicly shareable data by different government departments. [22] A national government-administered rural employment scheme was among several initiatives or agencies reported to have accidentally revealed Aadhaar numbers. [23] Additional breaches were reported in 2018 [24] and 2019. [25]

In September 2018, the Supreme Court ruled that Aadhaar is constitutional, but set important limits on the program's use. [26] The ruling held that the program is 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. It is unclear how the government and private companies utilizing Aadhaar data will implement the ruling, and what they will do with the Aadhaar user data they have.

Despite the court's restrictions on permissible uses of Aadhaar, the government promulgated the Aadhaar Ordinance in March 2019. The temporary ordinance allowed for the voluntary use of Aadhaar as proof of identity for bank accounts and mobile SIM connections, [27] and gave private companies access to some Aadhaar information they had been barred from after the Supreme Court judgment. In July 2019, Parliament passed the Aadhaar and Other Laws (Amendment) Bill, [28] a similar law

that supersedes the March 2019 ordinance. [29] Civil society groups have expressed serious concerns, arguing the bill ignores the 2018 Supreme Court ruling. [30] The law was challenged in the Supreme Court on the basis of provisions that allow private entities to use Aadhaar data provided voluntarily by customers for identity authentication. [31] As of July 2020, the case was pending.

In July 2018, the Srikrishna Committee, established in 2017 to create a data protection framework, [32] submitted a draft privacy framework for the Personal Data Protection Bill [33] and a report [34] to the MeitY. India's IT minister had stated that there would be consultations on the law [35] and that the cabinet and Parliament will further review the recommendations. [36] The Personal Data Protection Bill, 2019 was introduced in the lower house of Parliament in late 2019, with the bill referred to a Joint Parliamentary Committee. [37] As of July 2020, the bill remained pending.

The Personal Data Protection Bill, 2019 has been criticized widely, especially in relation to the extensive powers it gives to the central government, as well as its limited restrictions on surveillance activities by the government (see C6). [38] Claus 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." The bill provides for the establishment of a Data Protection Authority of India, but observers have raised issues regarding the prospective entity's independence, transparency, and accountability, given its composition, structure, and functions. [39]

In March 2020, it was reported that the government planned to build a large database called the National Social Registry that could track every Indian and allegedly capture a 360-degree view of their lives. The registry will include data captured in relation to any government services and benefits, including Aadhaar, and is expected to be functional by 2021. [40]

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 and other fundamental freedoms. [41] Government measures to counter the COVID-19 pandemic included the Aarogya Setu, a closed-source contact-tracing app, which was made mandatory for large sections of the population. [42] 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. Government agencies are permitted access to the centralized database that stores the data. The closed-source Quarantine Watch app, a Karnataka state government project, facilitates the enforcement of mandatory isolation by collecting detailed personal data, including GPS data and metadata linked to photographs users provide to prove their location. In addition, state and local authorities have rolled out a range of monitoring efforts during the pandemic, including drone surveillance, the publication of names and addresses of individuals under quarantine, and other smartphone apps. [43]

MeitY officials indicated that security agencies could access messaging services such as WhatsApp in 2017, though they are unable to view encrypted content. In response to a question in the lower house of Parliament, the IT minister stated that "security agencies are able to intercept these encrypted communication services through the lawful interception facilities provided by the Telecom Service Providers, but they are not able to decrypt some of encrypted intercepted communication to readable format." [44]

Evidence suggests that government and state agencies, including law enforcement, proactively monitor social media for signs of wrongdoing, although the legal grounds for doing so are unclear. In December 2018, a RTI request revealed that the Ministry of Information and Broadcasting had used a private firm to monitor social media for two years. [45] In another report from September 2018, both state and central government agencies were reported to be using Advanced Application for Social Media Analytics. [46] While detailed information about the sophistication of this technology is unclear, documents suggest that it uses sentiment analysis to categorize online content—such as "sensitive" information like protests (see B8)—as positive or negative, and can aggregate and analyze content and other data on social media platforms in real time. In

April 2018, the government announced plans to set up a Social Media Communication Hub and released a tender to purchase sophisticated monitoring technology. That August, the government withdrew the plans after the Supreme Court raised significant surveillance concerns over the monitoring. [47] 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 and detect disinformation and other types of false content. [48] The tender also requests the establishment of an archive for long-term data retention.

A special social media branch of the Mumbai police reportedly utilized an app to track behavioral patterns, analyze sentiments, and examine upticks in online chatter and conversation in order to generate real-time warnings and alerts. [49] In 2019, the Mumbai Police reported that they utilized the technique and worked with service providers and platforms to remove 12,537 objectionable posts from social media (see B2). [50]

**C6** 0-6 pts

| | |
|---|---|
| **Are service providers and other technology companies required to aid the government in monitoring the communications of their users?** | **2** / 6 |

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.

Eight separate intelligence bodies are authorized to issue surveillance orders to service providers. [1] Online intermediaries are required by law to “intercept, monitor, or decrypt” or otherwise provide user information to officials. [2] The Telegraph Act levies civil penalties or license revocation for noncompliance, [3] and violations of the IT Act carry a possible seven-year jail term. [4] Unlawful interception is punishable by just three years’ imprisonment. [5]

ISPs setting up cable landing stations are required to install infrastructure for surveillance and keyword scanning of all traffic passing through each

gateway. [6] 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; [7] and mandates prior approval from the DoT or a designated officer to install encryption equipment. [8]

In September 2018, the Supreme Court set new data retention requirements and called for the immediate passing of a "robust" data protection law. [9] However, a Personal Data Protection Bill intended to better protect privacy includes concerning provisions that could enable government surveillance without legislative backing (see C5). [10] The bill proposes a hybrid data localization model, raising concerns about surveillance and cybersecurity. [11] 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.

Standard Operating Procedures (SOP) for Lawful Interception and Monitoring of Telecom Service Providers—regulations issued in 2014 [12] —restricted interception to a service provider's "chief nodal officer," and mandated that interception orders be in writing. [13] Rules issued in 2011 under the IT Act provided for greater protection of personal data handled by companies, [14] but do not apply to the government.

The draft intermediary guidelines under Section 79 of the IT Act, which are designed to replace 2011 rules, would require intermediaries to retain any content removed for at least 180 days, or longer upon request by a court or a government agency (see B2). In the meantime, many components of the legal framework surrounding data retention and lawful interception remain inconsistent with one another.

License agreements require service providers to guarantee the designated security agency or licensor remote access to information for monitoring; [15] ensure that their equipment contains necessary software and hardware for centralized interception and monitoring; and provide the geographical location, such as the nearest Base Transceiver Station, of any subscriber at a given point in time. [16] Under a 2011 Equipment Security Agreement that did not appear on the DoT website, telecom

operators were separately told to develop the capacity to pinpoint any customer's physical location within 50 meters. [17] "Customers specified by security agencies" were prioritized for location monitoring, with "all customers, irrespective of whether they are the subject of legal intercept or not," to be monitored by June 2014. [18] The agreement apparently remains in effect.

In 2014, an amendment to licensing conditions mandated government testing for all telecom equipment prior to use, effective in 2015. [19] Cybercafé owners are required to photograph their customers, arrange computer screens in plain sight, keep copies of client identification and their browsing histories for one year, and forward this data to the government each month. [20]

In January and February 2020, local offices of the DoT reportedly made mass requests for call detail records of subscribers in various parts of the country, including Delhi, Andhra Pradesh, Haryana, Himachal Pradesh, Kerala, Odisha, Madhya Pradesh, and Punjab. These requests were reported after the COAI red-flagged the requests to the secretary of the DoT, noting that the requests did not conform to existing legal guidelines for such requests, including the required DoT rationale for seeking the information. [21]

The government also seeks user information from international tech platforms. Between July and December 2019, Google reported complying with 62 percent of the government's record-high 10,891 user data disclosure requests and 25,896 account access requests. [22] During the same time period, Facebook complied with 57 percent of the government's 26,698 requests for user data. [23] India made the second-highest number of such requests in the world, after only the United States. [24] In the same period, Twitter reported that it complied with 1.7 percent of the government's 789 requests for account information. [25]

**C7** 0-5 pts

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

Trolling and violent threats for online activity are common, as is physical violence during detentions and in politically tense circumstances such as protests.

During the CAA protests, online journalists faced physical violence and other forms of abuse from police, although much of the violence against journalists during the demonstrations related to offline reporting. [1] For example, Delhi police beat journalist Shaheen Abdulla of the news website Maktoob Media, a video of which was widely viewed on social media. [2] Journalists and activists have also faced physical violence and even alleged torture by authorities while in detention. [3] Activist Sadaf Jafar was arrested while live streaming to Facebook during the CAA protests, and she claimed that she was severely beaten by police during her time in detention. [4]

In February 2019, during the previous coverage period, Suman Pandey and Vinod Dongre, reporters for the online outlet The Voices, were attacked by local BJP members and forced to delete video footage while reporting on a “scuffle” at a BJP meeting. [5] In October 2018, Saritha Balan, from the online outlet the News Minute, was kicked by right-wing Hindu protestors while covering demonstrations against a Supreme Court ruling allowing women of all ages to enter the Sabarimala temple in Kerala. [6]

Aggressive online commentators who self-identify as Hindu nationalists routinely abuse their opponents. Much trolling appears to align with the BJP governing agenda, but there is limited evidence that government actors are directly involved. Rather, officials’ tacit support of online abuse—evidenced, for example, by the prime minister following known troll accounts on Twitter, or the use of volunteers to pump out anti-Muslim content across WhatsApp ahead of the elections—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. [7]

However, in some cases BJP officials have directly disseminated incendiary content or other violent threats online. The *Wall Street Journal*

reported in August 2020, after the coverage period, that BJP politician T. Raja Singh's violent and Islamophobic content on Facebook, including calls for Rohingya Muslims to be shot, violated the company's policies. [8] In another instance, Arfa Khanum Sherwani, a senior editor at the Wire, was subjected to online harassment, bullying, and death and rape threats on social media by BJP officials in January and February 2020. [9]

Reports suggest that these forms of abuse and trolling are heightened when the victim is a woman, a Muslim or member of another minority religion, is from a lower caste, or otherwise identifies within a marginalized group. [10] Journalists are also targeted on social media irrespective of the medium they work in. For example, journalist Rana Ayyub has been the target of death and rape threats on social media. [11]

Hate speech against Muslims is rampant on Twitter, with Islamophobic hashtags frequently trending. In October 2019, a hashtag in Hindi that translated to "Total Boycott of Muslims" trended in the country. [12] In April 2020, the hashtag "CoronavirusJihad" began trending on Twitter as false information claiming the Muslim community was spreading the disease circulated widely. [13] Member of Parliament and BJP official Anantkumar Hedge reportedly shared similar content on Facebook. [14]

Women in politics commonly experience trolling. [15] In June 2018, a barrage of users attacked, using misogynistic and hateful language, then Minister of External Affairs Sushma Swaraj for helping an interfaith couple obtain a passport. [16] 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. [17] An Amnesty report states 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. Women from marginalized communities faced the brunt of the abuse: Muslim women faced 94 percent more ethnic and religious slurs, and women from Bahujan backgrounds received 59 percent more caste-based abuse compared to women from privileged upper-caste backgrounds. [18]

As newer platforms like TikTok gained in popularity in India, they become another source for online harassment of people from minority groups and particular castes. [19] In some cases, this led to consequences such as suicide and physical violence. A Wired report in mid-2019 noted that across a two-month time period, 500 pieces of casteist content, in the form of hate speech and threats of violence and abuse, were identified on TikTok. Caste names of certain communities served as the hashtags under which large volumes of abusive content were generated. [20]

**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) reported nearly 395,000 cybersecurity incidents in 2019, almost double the figure from 2018. [1] Over 305,000 of these attacks were network scanning, probing, or vulnerable services. Another 62,163 were incidents related to a virus or malicious code, while just over 24,366 were website defacements. CERT-In issues periodic advisories, and the government updates a crisis-management plan for central and state governments to respond to cybercrime on an annual basis. [2] CERT-In also established that 35 percent of attacks against India were orchestrated by China. [3]

Reports suggest that cybersecurity attacks and breaches increased dramatically in India since the beginning of the COVID-19 lockdown in March 2020. [4] In April 2020, amid the pandemic, hackers linked to Pakistan reportedly posed as government health advisors to send malware-containing emails to many Indian citizens in an attempt to gain access to personal information. [5] 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. [6]

In June 2020, after the coverage period, hackers allegedly based in China reportedly attempted 40,300 cyberattacks across five days amid a spike in border dispute-related tensions between China and India. [7] The attacks were aimed at hijacking internet protocols and phishing.

A report by the software solutions provider Subex said India suffered the world's highest number of cyberattacks during the second quarter of 2019, with spikes coinciding with geopolitical tensions in the region. [8] Critical infrastructure bore the brunt of these attacks, with sensitive sectors such as banking and defense also affected.

According to Symantec's 2018 Internet Security Threat Report, India was subject to the second-highest number of targeted attacks in the world between 2015 and 2017. [9] The UK-based Comparitech rated India as the 18th least cyber-secure nation in 2020, an improvement from the country's rank of 15 in 2019. [10]

**On India**

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

See More ›

***Country Facts***

Global Freedom Score

**71** /100 **Free**

Internet Freedom Score

**51** /100 **Partly Free**

Freedom in the World Status

**Free**

Networks Restricted

**Yes**

Social Media Blocked
**No**

Websites Blocked
**Yes**

Pro-government Commentators
**Yes**

Users Arrested
**Yes**

***In Other Reports***

Freedom in the World 2020

***Other Years***

2019




ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org