GROWTH OF DIGITAL RESTRICTIONS IN INDIA:

Spotlight on Surveillance and Other Threats to Free Expression

Resource paper for the
International Center for Not-for-Profit Law (ICNL)

PUBLISHED NOVEMBER 2022

GROWTH OF DIGITAL RESTRICTIONS IN INDIA:

Spotlight on Surveillance and other Threats to Free Expression

Published in November 2022

Table of Contents

I. Introduction

Digital civic space in India is shrinking. Reports by organisations such as CitizenLab and Amnesty International as well as private firms such as Arsenal Consulting and SentinelOne have showcased the increasing illegal targeting and surveillance of civil society actors in India through spyware, including the recent Pegasus scandal.[1] Meanwhile, ongoing attacks on journalists such as Mohammed Zubair, co-founder of the Indian fact checking website Alt News, and others who challenge accepted mainstream narratives, exemplify the growing threat to digital rights and civil liberties.[2] There have been significant increases in hate speech and disinformation, while minority actors, vulnerable or marginalized groups, women and human rights defenders are consistently subjected to censorship.[3]

The following briefer focuses on these growing digital threats, examining the proliferation of illegal surveillance in recent years, as well as representative examples of the suppression of free expression online for civil society actors. It includes recent examples of concerning surveillance trends, the failure to curb disinformation, and tolerance of hate speech. Collectively, these digital restrictions are having chilling effects on civil society and India's free and open democratic discourse.

1 "Forensic Methodology Report: How to Catch NSO Group's Pegasus" (Amnesty International, July 18, 2021), https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/; see also Andy Greenberg, "Police Linked to Hacking Campaign to Frame Indian Activists," Wired, accessed June 27, 2022, https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/.

2 Zubair has been a target of rising intolerance in the country with multiple police complaints registered against him for speech online, one of which resulted in his arrest and threats of violence. "Journalist Mohammed Zubair Booked for Calling Hate Speech Accused Seers 'Hatemongers,'" Scroll.in, accessed June 23, 2022, https://scroll.in/latest/1025282/alt-news-co-founder-mohammed-zubair-booked-for-calling-hindu-supremacists-hatemongers.

At least 7 journalists were jailed in India in 2021. In addition to these actions by state authorities, journalists have also been victims of physical violence, with at least 4 have been killed recently. "Committee to Protect Journalists – Defending Journalists Worldwide.," *Committee to Protect Journalists*, accessed June 21, 2022, https://cpj.org/data/imprisoned/2021/?status=Imprisoned&cc_fips%5B%5D=IN&start_year=2021&end_year=2021&group_by=location; "Attacks on the Press: The Deadliest Countries in 2021," *Committee to Protect Journalists*, accessed June 21, 2022, https://cpj.org/reports/2022/01/attacks-on-the-press-the-deadliest-countries-in-2021/.

3 Physical instances of hate and violence are amplified online through increased hate speech and disinformation on platforms, which are often then linked to further instances of physical violence, resulting in the cyclical propagation of hate and violence, with digitisation playing an important role in furthering these harms. See, e.g., Maya Mirchandani, "Digital Hatred, Real Violence: Majoritarian Radicalisation and Social Media in India" (Observer Research Foundation, August 29, 2018), https://www.orfonline.org/research/43665-digital-hatred-real-violence-majoritarian-radicalisation-and-social-media-in-india/.

II. The Spread of Overbroad and Illegal Surveillance in India

The existing gaps in the Indian surveillance framework – and evidence that state-sponsored surveillance has occurred – present a major roadblock towards India's commitment to upholding privacy and freedom of expression.[4]

Today, it is possible for spyware to hack a person's electronic device and access all messages, contacts, emails, and photographs, as well as activate the device's microphone or camera and enabling recording. This advancement in technology has outpaced legal regulations. The Indian regulatory framework lacks safeguards against illegal or over-intrusive surveillance, allowing the use of such technology without oversight or accountability. This raises serious concerns since the deployment of surveillance technology to target journalists, activists, and human rights defenders has already commenced in India. In the absence of privacy and data protections, such surveillance creates a chilling effect where individuals are afraid to freely express themselves.

A. Problems with the Existing Surveillance Framework in India

The existing surveillance framework in India consists of Section 5(2) of the Indian Telegraph Act, 1885 and Section 69 of the IT Act which find process and procedure as per Rule 419-A of the Telegraph Rules, 1951 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 respectively. Section 5(2) of the Indian Telegraph Act and supporting rules regulate the interception of calls while Section 69 of the IT Act and supporting rules regulate the interception of data. In addition to these provisions and supporting rules, there exists a "Standard Operating Procedure" for interception, handling, sharing, copying, storage, and destruction of messages/telephones issued by the Ministry of Home Affairs on May 19, 2011.[5]

Under the surveillance framework, calls can only be intercepted during a public emergency or in the interest of public safety, while interception of data does not have any such specific restriction. Interception of data may be carried out for reasons

4 "'Govt Committed to Right to Privacy': India's Response over Pegasus Hack," *Hindustan Times*, July 18, 2021, https://www.hindustantimes.com/india-news/govt-committed-to-right-to-privacy-india-s-response-over-pegasus-hack-101626631762226.html; see also Shubhajit Roy, "India Joins G7, 4 Others to Protect Free Speech, 'Online and Offline,'" *The Indian Express*, June 28, 2022, https://indianexpress.com/article/india/india-joins-g7-4-others-to-protect-free-speech-online-and-offline-7994867/.

5 "'Standard Operating Procedure' for Interception, Handling, Sharing, Copying, Storage, and Destruction of Messages/Telephones" (Ministry of Home Affairs, May 19, 2011), https://drive.google.com/file/d/1CAuUWKywa6EGTnh5w5r5JqipeF8zIY9C/view?usp=sharing.

related to the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order and preventing incitement to the commission of an offence. The power of authorisation for any surveillance activity lies with the Central or State Government, or any officer authorised on their behalf.[6]

Certain concerns arise with respect to this framework. Firstly, these grounds have not been specifically defined, allowing for vague and arbitrary interpretations in individual instances of surveillance. Secondly, the power to authorise and monitor surveillance activities is concentrated in the hands of the executive; there is no judicial or parliamentary oversight over the actions of the executive when it comes to instances of surveillance.[7] The only oversight is provided by a Review Committee, consisting solely of members from the executive, which is authorised to order destruction of intercepted messages if it finds the interception to not be in accordance with the relevant provisions. According to leading IT researchers, "in the absence of judicial or legislative oversight, such powers result not only in a disproportionate restriction on individual fundamental right to privacy, but also have far-reaching consequences for other freedoms – a chilling effect on the freedom of speech and association and democratic participation".[8]

Since surveillance by its very nature is carried out in secrecy, and there is no obligation upon the government to inform the surveilled person of its actions at a later stage, there is little opportunity for relief under Articles 32 or 226 of the Constitution (which empower the Supreme Court and High Courts in India to issue certain writs) or any other recourse in the event of overbroad surveillance. Thus, while the existing surveillance framework does define certain conditions and grounds for carrying out surveillance, these are essentially

Since surveillance by its very nature is carried out in secrecy, and there is no obligation upon the government to inform the surveilled person of its actions at a later stage, there is little opportunity for relief under the Constitution.

6 Chaitanya Ramachandran, "PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Revised for the Digital Age – NUJS Law Review," NUJS Law Review 7, no. 2 (2014), http://nujslawreview.org/2016/12/04/pucl-v-union-of-india-revisited-why-indias-surveillance-law-must-be-revised-for-the-digital-age/.

7 Vrinda Bhandari and Karan Lahiri, "The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World," *Univ. of Oxford Human Rights Hub Journal* 15, no. 2020 (April 20, 2020), https://papers.ssrn.com/abstract=3580630.

8 Tathagata Satpathy, Karnika Seth, and Anita Gurumurthy, "Are India's Laws on Surveillance a Threat to Privacy?," *The Hindu*, December 28, 2018, sec. Comment, https://www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25844250.ece.

legal fictions, since there are no checks in place to ensure that they are being followed.

The fear of overbroad surveillance is no longer hypothetical. According to a 2013 right to information request response, the Central Government issues 7500 to 9000 interception orders on an average per month.[9] It is safe to assume that it is almost impossible for a review committee to properly consider and effectively evaluate the legality of almost 9000 interception orders per month.[10] Interception is therefore likely being approved without proper oversight, leading to violations of the fundamental rights of citizens.

In addition to the Indian surveillance framework being overbroad and opaque, it is also outdated. The existing framework only consists of provisions related to targeted surveillance via interception of calls and data. However, surveillance technology has advanced much further, advancements for which there are no corresponding legal provisions in the Indian surveillance framework.

B. Ongoing Use of Advanced Technology to Carry Out Targeted Surveillance Against Civil Society

In 2021, 17 news media organisations came together for the Pegasus Project, a collaborative investigative project. The project revealed that an Israeli spyware firm, NSO Group, was using its spyware, Pegasus, to potentially target "over 300 verified Indian mobile telephone numbers, including those used by ministers, opposition leaders, journalists, the legal community, businessmen, government officials, scientists, rights activists and others".[11] This was not the first time that use of Pegasus had been uncovered in India. However, while in 2019 Pegasus needed some action on the part of the targeted person to infect their device, the updated spyware used in 2021 had the capability to conduct 'zero-click' attacks.[12]

Rupesh Kumar Singh, an independent journalist, and Ipsa Shatakshi, an activist, are two individuals whose phones were targeted by the Pegasus spyware. In August 2021, they approached the Supreme Court of India requesting that the Court declare the use of Pegasus on Indian citizens unconstitutional.[13] The Court subsequently constituted a technical committee to examine the allegations made with regard to use of Pegasus in

9 "RTI Reveals as Many 9000 Phones, 500 e-Mails Intercepted Each Month during UPA," accessed July 5, 2022, https://www.aninews.in/news/national/general-news/rti-reveals-as-many-9000-phones-500-e-mails-intercepted-during-upa20181222180444000 1/.

10 "HC Asks CIC to Decide within Eight Weeks Appeal against MHA's Refusal to Give Info on e-Surveillance," *The Economic Times*, December 2, 2021, https://economictimes.indiatimes.com/news/india/hc-asks-cic-to-decide-within-eight-weeks-appeal-against-mhas-refusal-to-give-info-on-e-surveillance/articleshow/88051529.cms?from=mdr.

11 Siddharth Varadarajan, "Pegasus Project: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy On Them," The Wire, July 18, 2021, https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying.

12 "WhatsApp Confirms: Israeli Spyware Was Used to Snoop on Indian Journalists, Activists," *The Indian Express* (blog), November 1, 2019, https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/.

13 "Pegasus-Affected Journalists, Activist Move SC, Want Govt to Come Clean on Spyware Use," The Wire, March 8, 2021, https://thewire.in/law/five-journalists-move-sc-wants-centre-to-disclose-if-it-authorised-use-of-pegasus.

India.[14] As part of its investigation, the Committee examined 29 phones alleged to have been targeted by Pegasus, and sought responses from the public regarding the existing lacunae in the Indian surveillance framework.[15]

Since these revelations were made, similar instances of the illegal use of surveillance technology in India have come to light. Arsenal Consulting, a digital forensics consulting firm, analysed electronic evidence seized from two activists accused of criminal activity, who were part of the Bhima Koregaon 16, a group of 16 prominent activists, intellectuals, social workers, lawyers, and cultural artists, many of whom worked for Dalit rights.[16] In its reports from early 2021, Arsenal concludes that the evidence forming the basis of the case against both activists (Rona Wilson and Surendra Gadling) was planted through a commercially available spyware called NetWire for almost two years before their arrests.[17] Further, security firm SentinelOne has linked this hacking to the Pune Police, which made the original arrests in the Bhima Koregaon incident.[18]

While the Pegasus and Netwire allegations relate to specific instances of targeted surveillance of human rights defenders and journalists, a 2021 threat report by Meta-Facebook also reveals the existence of a growing hack-for-hire industry in India.[19] The report identified seven entities who were involved in hack-for-hire activities globally and subsequently removed from Facebook platforms. One of these was an Indian entity,

A 2021 threat report by Meta-Facebook also reveals the existence of a growing hack-for-hire industry in India. The report identified seven entities who were involved in hack-for-hire activities globally and subsequently removed from Facebook platforms.

14 Krishnadas Rajagopal, "Supreme Court Forms Committee to Examine Pegasus Allegations," *The Hindu*, October 27, 2021, sec. National, https://www.thehindu.com/news/national/supreme-court-judgment-on-pegasus/article37184269.ece.

15 Krishnadas Rajagopal, "29 Phones Tested for Pegasus Spyware: Supreme Court," *The Hindu*, May 20, 2022, sec. National, https://www.thehindu.com/news/national/pegasus-case-sc-grants-more-time-to-probe-panel-29-mobiles-being-examined-for-spyware/article65438682.ece; see also "SC-Appointed Pegasus Probe Committee Seeks Responses from Public on 11 Queries," The Wire, March 25, 2022, https://thewire.in/law/sc-appointed-pegasus-probe-committee-seeks-responses-from-public-on-11-queries.

16 Included among the 16 defendants accused was 84-year-old Jesuit priest and human rights defender Stan Swamy, who died in jail last year after contracting COVID-19.

17 Niha Masih and Joanna Slater, "Evidence Found on a Second Indian Activist's Computer Was Planted, Report Says," *Washington Post*, June 7, 2021, https://www.washingtonpost.com/world/2021/07/06/bhima-koregaon-case-india/.

18 Andy Greenberg, "Police Linked to Hacking Campaign to Frame Indian Activists," *Wired*, June 16, 2022, https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/.

19 David Agranovich and Mike Dvilyanski, "Taking Action Against the Surveillance-For-Hire Industry," *Meta* (blog), December 16, 2021, https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/.

Belltrox Infotech Services Private Limited ('Belltrox').[20] Belltrox has also been identified as an "Indian cyber mercenary" that was "hacking parties involved in lawsuits around the world" by a 2022 Reuters Special Report.[21]

The prevalence of hacking and targeted surveillance demonstrates the extent to which entities are exploiting the gaps that exist in the Indian surveillance framework. However, while some legal provisions around targeted surveillance, even if inadequate, do exist, the Indian surveillance framework has entirely failed to acknowledge and respond to the growing threat of *mass* surveillance in the country.[22]

C. The Looming Threat of State-Sponsored Mass Surveillance to Civic Freedoms

In India, the building blocks of mass surveillance – the indiscriminate data gathering of entire populations – are the increasingly high number of Close Circuit Television cameras (CCTVs) being deployed throughout the country. In recent years, Indian cities have raced ahead in CCTV deployment. According to a 2021 Comparitech report (updated in July 2022), Delhi is the most surveilled city in the world in terms of cameras per square mile, while Indore is the second most surveilled city in the world in terms of cameras per person, just behind cities in China.[23] The dominant rhetoric surrounding the increased deployment of CCTVs is that they assist in crime reduction, a coveted outcome for governments in India. However, multiple studies reveal that there is little correlation between CCTV deployment and crime reduction in an area.[24] What then is the purpose of CCTV deployment? According to one scholar, CCTVs are quite effective in carrying out other aspects of policing, especially relating to restoring the 'normative order' (the local, authoritative conceptions of order), as a result of which CCTV surveillance often disproportionately targets minority communities and those who have been deemed as the "other" or anything threatening the normal order.[25]

In addition to enabling the continuous monitoring of any individual who comes under

20 Ryan Gallagher, "Meta Identifies Six Firms, Including India's BellTroX, for Spying on Users," *Business Standard India*, December 17, 2021, https://www.business-standard.com/article/current-affairs/meta-identifies-six-firms-including-india-s-belltrox-for-spying-on-users-121121700159_1.html.

21 Raphael Satter, "How Mercenary Hackers Sway Litigation Battles," Reuters Special Report (Reuters, June 30, 2022), https://www.reuters.com/investigates/special-report/usa-hackers-litigation/.

22 For the sake of clarity, the difference between targeted and mass surveillance is that under targeted surveillance, specific people are spied upon, i.e., targeted, while under mass surveillance, entire populations are surveilled indiscriminately.

23 Paul Bischoff, "Surveillance Camera Statistics: Which City Has the Most CCTV Cameras?," Surveillance Studies (Comparitech, May 7, 2022), https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

24 "Does Increased CCTV Surveillance Help Reduce Crime? Not Really," Mintlounge, January 7, 2021, https://lifestyle.livemint.com//news/talking-point/does-increased-cctv-surveillance-help-reduce-crime-not-really-111609944751428.html; see also Brandon C. Welsh and David P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime," *Campbell Systematic Reviews* 4, no. 1 (January 2008): 1–73, https://doi.org/10.4073/csr.2008.17; Jayant Pankaj, "CCTV Surveillance Is Rising in India, World, but Crime Rates Remain Unaffected," The Wire, May 1, 2022, https://thewire.in/rights/cctv-surveillance-is-rising-in-india-world-but-crime-rates-remain-unaffected.

25 Aaron Doyle, Randy Lippert, and David Lyon, eds., *Eyes Everywhere | The Global Growth of Camera Surveillance*, 1st ed., 2011, https://www.taylorfrancis.com/books/edit/10.4324/9780203141625/eyes-everywhere-aaron-doyle-randy-lippert-david-lyon.

their gaze and disproportionately affecting historically overpoliced communities, CCTVs also gather data for the more advanced surveillance technologies such as facial recognition, emotion recognition, and other AI-based surveillance technologies.[26] The use of facial recognition technology has increased at an unprecedented rate in India. According to Internet Freedom Foundation's Project Panoptic, which maps the growth of facial recognition use by government authorities in India, government authorities are developing and deploying approximately 124 facial recognition systems.[27] The use of facial recognition is especially concerning when carried out by law enforcement authorities for investigation purposes, since it can have severe consequences on fundamental rights, lead to bias & discrimination, and enable mass surveillance.[28]

Nonetheless, the use of facial recognition technology (FRT) by law enforcement in India continues. The Delhi Police acquired FRT through a decision of the Delhi High Court which said that the Police may use facial recognition to find missing children.[29] However, through a massive over-extension of this mandate, the Delhi Police have been reported to have used FRT on protesters during the Anti-Citizenship Amendment Act (CAA) protests in 2019, as well as during the 2020-2021 farmers' protests.[30] The Delhi Police also used facial recognition to allegedly identify "rioters" during the 2020 North East Delhi Riots and the 2021 Republic Day Parade violence at the Red Fort. According to multiple reports, FRT was used in 137 of the 1,800 arrests in the North East Delhi riots and over 250 people were identified through facial recognition for the Red Fort violence.[31] Outside of these specific incidents, the Delhi Police have arrested 42 people with the help of facial recognition systems since the technology was introduced in August 2020, conducting a total of 18,968 FRT scans between August 2020 and March 2021.[32]

With over 600,000 CCTV cameras deployed, all of which connect to a Command & Control Centre containing multiple artificial intelligence (AI)-enabled surveillance technologies, the city of Hyderabad in the state of Telangana is fast becoming one of

26 Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy" (American Civil Liberties Union, June 2019), https://www.aclu.org/report/dawn-robot-surveillance.

27 "Project Panoptic" (Internet Freedom Foundation), accessed July 7, 2022, https://panoptic.in.

28 Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up" (Centre for Privacy & Technology, Georgetown Law, October 18, 2016), https://www.perpetuallineup.org/.

29 "Delhi: Facial Recognition System Helps Trace 3,000 Missing Children in 4 Days," *Times of India*, April 22, 2018, https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms.

30 Alexandra Ulmer and Zeba Siddiqui, "India's Use of Facial Recognition Tech during Protests Causes Stir," *Reuters*, February 17, 2020, sec. Emerging Markets, https://www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ; see also Mehab Qureshi, "Can Face Recognition Technology Identify Farmer Protesters?," TheQuint, January 28, 2021, https://www.thequint.com/tech-and-auto/can-facial-recognition-technology-identify-farmer-protesters.

31 Jignasa Sinha, "Face Recognition Software Used in 137 of 1,800 Arrests in Northeast Delhi Riots, Says Police," *The Indian Express*, February 20, 2021, https://indianexpress.com/article/cities/delhi/delhi-riots-police-cctv-7196291/; see also "Facial Recognition Tool Used to Identify Red Fort Raiders," *The Economic Times*, January 29, 2021, https://economictimes.indiatimes.com/news/politics-and-nation/facial-recognition-tool-used-to-identify-red-fort-raiders/articleshow/80516165.cms.

32 Aman Dwivedi, "Facial Recognition System Behind 42 Arrests Since August: Delhi Police," NDTV.com, January 4, 2021, https://www.ndtv.com/delhi-news/facial-recognition-system-behind-42-arrests-since-august-delhi-police-2403950.

the most surveilled cities in India.[33] The Hyderabad Police have also drawn scrutiny for their excessive use of surveillance technology, which has resulted in India's first court challenge to the use of the technology by police.[34] In addition to Delhi and Hyderabad, many other state police departments have also acquired the technology. However, in an attempt to streamline the process nationally, the Indian Ministry of Home Affairs is developing a National Automated Facial Recognition System (AFRS), touted to be the world's largest facial recognition system.[35]

The AFRS is just one example of the multiple large-scale surveillance systems that the Government has put in place since 2008. Other instances include: the National Intelligence Grid (NatGRID), which provides an information sharing platform between the intelligence agencies and e-governance organisations in India;[36] the Crime and Criminal Tracking Network System (CCTNS), which aims to create "a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals'";[37] the Centralised Monitoring System (CMS), which "gives India's security agencies and income tax officials centralised access to the country's telecommunications network";[38] and the Networking Traffic Analysis (NETRA), which is a "real time surveillance software… meant to monitor internet traffic on a real time basis using both voice and textual forms of data communication, especially social media, communication services and web browsing".[39]

All of these systems operate in the absence of any legal framework which would regulate their operations and establish effective legal safeguards to protect against misuse. While the Supreme Court held privacy to be a fundamental right flowing from the right to life in the Constitution in 2017, there is no specific law enshrining the right.[40] The Personal Data Protection Bill, 2019 has languished in parliamentary deliberations for

33 "Ban the Scan: Hyderabad" (Amnesty International), accessed July 7, 2022, https://banthescan.amnesty.org/hyderabad/.

34 Rina Chandran, "Surveillance Hotspot, Hyderabad, Sees Facial Recognition Taken to Court," *The Economic Times*, January 21, 2022, https://economictimes.indiatimes.com/news/india/surveillance-hotspot-hyderabad-sees-facial-recognition-taken-to-court/articleshow/89007252.cms?from=mdr.

35 Julie Zaugg, "India Is Trying to Build the World's Biggest Facial Recognition System," CNN, October 18, 2019, https://edition.cnn.com/2019/10/17/tech/india-facial-recognition-intl-hnk/index.html.

36 D. Haritha and Ch. Praneeth, "National Intelligence Grid — An Information Sharing Grid," in *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, 2017, 1–6, https://doi.org/10.1109/ICAMMAET.2017.8186674.

37 "Crime and Criminal Tracking Network & Systems (CCTNS)," National Crime Records Bureau, accessed July 7, 2022, https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns.

38 Maria Xynou, "India's Central Monitoring System (CMS): Something to Worry About? — The Centre for Internet and Society," The Centre for Internet & Society, January 30, 2014, https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

39 Udbhav Tiwari, "The Design & Technology behind India's Surveillance Programmes — The Centre for Internet and Society," The Centre for Internet & Society, January 20, 2017, https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes.

40 Jyoti Panday, "India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time," Electronic Frontier Foundation, August 28, 2017, https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.

the past four years.[41] Lawmakers are no closer to addressing expert criticisms of the Bill, including the government's overbroad exemptions and a failure to safeguard user rights and consent.[42] These exemptions would have effectively allowed the government to exempt all agencies that carry out surveillance from the purview of the data protection legislation, resulting in continued vulnerability of citizen privacy.[43] However, on August 3, 2022, the draft Data Protection Bill was withdrawn to purportedly make way for a comprehensive legal framework for the digital ecosystem.[44]

It is apparent that in the absence of any effective regulatory framework, the current surveillance technology in use in India remains unchecked and could lead to mass privacy violations and continued targeting of civil society actors. Spyware like Pegasus has been used to target civil society actors and place incriminating materials on their devices, while facial recognition technology continues to be used to arrest protesters and suppress social movements. Given the lack of adequate safeguards, there seems a very real risk that surveillance technology in India will continue to be used to suppress civic freedoms and other human rights.

In the absence of any effective regulatory framework, the current surveillance technology in use in India remains unchecked and could lead to mass privacy violations and continued targeting of civil society actors.

41 Its journey started on July 27, 2018, when the Justice BN Srikrishna Committee submitted its report to the Ministry of Electronics and Information Technology. The scope of the Committee was to "examine issues related to data protection, recommend methods to address them, and draft a data protection Bill" which it did by proposing the Draft Personal Data Protection Bill, 2018. The Bill was then introduced in the Indian Parliament as the Draft Personal Data Protection Bill, 2019, which was subsequently sent to a Joint Parliamentary Committee (JPC) in December, 2019. In December 2021, the JPC submitted its report which contained an updated version of the Bill termed as the Data Protection Bill, 2021 (DPB, 2021).

42 Clause 35 of the DPB, 2021 allowed the Central Government to exempt any government department from the application of the Bill. The Clause only required the procedure through which such exemption is granted to be 'just, fair, reasonable and proportionate', instead of the conditions which have to be met to grant such an exemption. Apar Gupta and Vrinda Bhandari, "National Security, at the Cost of Citizens' Privacy," *The Indian Express*, December 20, 2021, https://indianexpress.com/article/opinion/columns/national-security-at-the-cost-of-citizens-privacy-7680787/.

43 Deeksha Bhardwaj, "Data Protection Bill: Five MPs File Dissent Notes in Final Report," Hindustan Times, November 23, 2021, https://www.hindustantimes.com/india-news/data-protection-bill-five-mps-file-dissent-notes-in-final-report-101637606270285.html.

44 "Government Withdraws Data Protection Bill, 2021," *The Economic Times*, August 3, 2022, https://economictimes.indiatimes.com/tech/technology/government-to-withdraw-data-protection-bill-2021/articleshow/93326169.cms?from=mdr.

III. Increased Disinformation and Hate Speech

While India still has a significant digital divide, access to the internet has increased in recent years, especially during the pandemic when reliance on the internet for basic needs grew. The Government has implemented programs to increase internet access, such as the Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) scheme which aims to make six crore (60 million) people in rural areas 'digitally literate'.[45] According to the Telecom Regulatory Authority of India's (TRAI) Yearly Performance Indicators Report for 2021, the total internet subscribers in India have increased from 795.18 million in 2020 to 829.30 million in 2021, with an overall internet penetration of 60.46%.[46]

Unfortunately, increased internet access has made it easier for certain actors to spread disinformation and hate speech.[47] Fearmongering speech and false rumours are shared widely on platforms like Whatsapp, which further the radicalisation of those who are exposed to them.[48] Whatsapp, whose largest customer base is in India, has emerged as one of the leading platforms for the spread of hate speech as well as disinformation, with reports suggesting it was used to plan violent attacks on Muslims during the riots that took place in Delhi in February 2020.[49] Facebook in India has similarly been found to be "selective in curbing hate speech, misinformation and inflammatory posts, particularly anti-Muslim content".[50]

Digital media and online platforms also play a significant role in spreading divisive propaganda leading to communal violence, among other real world harms.[51] In India, online publications such as Opindia and Swarajya Magazine routinely peddle disinformation directed at minorities.[52] According to John Brittas, a journalist and

45 "Overview of PMGDISHA – Pradhan Mantri Gramin Digital Saksharta Abhiyan," accessed July 8, 2022, https://www.pmgdisha.in/about-pmgdisha/.

46 "Yearly Performance Indicators of Indian Telecom Sector - 2021" (Telecom Regulatory Authority of India, August 7, 2022), https://www.trai.gov.in/release-publication/reports/performance-indicators-reports.

47 "Hate Speech Faced by Indian Online Users Doubled in Last 4 Years: Microsoft," The News Minute, February 10, 2021, https://www.thenewsminute.com/article/hate-speech-faced-indian-online-users-doubled-last-4-years-microsoft-143138.

48 Punyajoy Saha et al., "'Short Is the Road That Leads from Fear to Hate': Fear Speech in Indian WhatsApp Groups" (arXiv, February 7, 2021), http://arxiv.org/abs/2102.03870; see also Kiran Garimella and Dean Eckles, "Images and Misinformation in Political Groups: Evidence from WhatsApp in India" (arXiv, May 19, 2020), http://arxiv.org/abs/2005.09784.

49 Vijayta Lalwani and Shoaib Daniyal, "From Planning Murder to Praising Modi: WhatsApp Chats Offer a Window into the Minds of Delhi Rioters," Text, Scroll.in (https://scroll.in, July 9, 2020), https://scroll.in/article/966775/from-planning-murder-to-praising-modi-whatsapp-chats-offer-a-window-into-the-minds-of-delhi-rioters.

50 Associated Press, "Facebook dithered in curbing divisive user content in India," October 23, 2021, https://www.npr.org/2021/10/23/1048746697/facebook-misinformation-india.

51 Zainab Sikander, "Islamophobia in Indian Media," *Islamophobia Studies Journal*, October 1, 2021, https://doi.org/10.13169/islastudj.6.2.0120.

52 Chaudhari, "Sudarshan News and Its History of Dangerous, Communally-Divisive Misinformation," Alt News, October 23, 2019, https://www.altnews.in/sudarshan-news-and-its-history-of-dangerous-communally-divisive-misinformation/; see also Basant Kumar, "Fake News, Lies, Muslim Bashing, and Ravish Kumar: Inside OpIndia's Harrowing World," Newslaundry, accessed June 28, 2022, https://www.newslaundry.com/2020/01/03/fake-news-lies-muslim-bashing-and-ravish-kumar-inside-opindias-harrowing-world.

member of Parliament, "(t)he role that the Indian media …has played in mainstreaming hate speech and divisive nationalism since 2014 is a topic that warrants a larger study".[53]

For instance, while OpIndia claims to be a "news and current affairs website," analysis by an independent news media company alleges there have been at least 25 instances of false news and no less than 14 instances of misreporting by OpIndia.[54] One such report relates to the death of a Hindu boy due to drowning in Gopalganj, Bihar. Multiple reports in OpIndia claimed that the boy was sacrificed in a mosque by the suspects in the boy's death, who OpIndia made a point of noting were all Muslim. However, fact checks established that the boy's death was in fact due to drowning after he and the suspects, who in actuality included another Hindu boy, finished playing cricket and went for a dip in the nearby river.[55]

Instead of appropriate action being taken against such online channels and publications, their talking points are often shared and endorsed by politicians in power.[56] Vilifying the 'other' through public speeches—essentially one-way conversations with little opportunity for rebuttal of falsehoods—allows propaganda to spread unchecked, especially in the age of social

Instead of appropriate action being taken against such online channels and publications, their talking points are often shared and endorsed by politicians in power.

53 John Brittas, "Media Must Be Held Accountable for Mainstreaming Hate Speech, Divisive Nationalism," *The Indian Express*, June 10, 2022, https://indianexpress.com/article/opinion/columns/media-in-the-dock-7959679/.

54 NewsLaundry, "OpIndia – A Dossier on False News and Misreporting," accessed June 28, 2022, https://docs.google.com/spreadsheets/d/1KZ8uboNOOhGztxSMMJOHk5T7rP2IuBOdHya5yWxuE_8/edit?usp=sharing&usp=embed_facebook.

55 Basant Kumar, "'Human Sacrifice in Mosque': How OpIndia Communalised a Bihar Boy's Death," Newslaundry, accessed June 28, 2022, https://www.newslaundry.com/2020/05/19/human-sacrifice-in-mosque-how-opindia-communalised-a-bihar-boys-death. OpIndia also routinely communalises news reports through their headlines, especially related to any incident of crime where even one suspect belongs to the Muslim community. This practice was illustrated by the headline for the report related to the 2019 rape and murder of a Hyderabad based veterinarian. Of the 4 suspects, 3 belonged to the Hindu community, however OpIndia chose to run the headline, "Mohammad Pasha had planned the rape and murder of Disha and burnt the body, police claim", focusing attention only on the sole Muslim suspect.

56 Liz Matthew and Abhinav Rajput, "Minister Anurag Thakur Chants Desh Ke Gaddaron Ko, Poll Rally Crowd Completes Goli Maaro…," *The Indian Express*, January 28, 2020, https://indianexpress.com/article/india/anurag-thakur-slogan-rithala-rally-6238566/;. Praneet Pathak, "Has AAP Taken Another Leap to Embrace Communal Politics?," The Wire, April 26, 2022, https://thewire.in/politics/has-aap-taken-another-leap-to-embrace-communal-politics; see also Sanjay Jog, "FIR Lodged against Shiv Sena's Ramdas Kadam for Hate Speech," *Business Standard India*, April 23, 2014, https://www.business-standard.com/article/elections-2014/fir-lodged-against-shiv-sena-s-ramdas-kadam-for-hate-speech-114042300499_1.html.

media, where 'explosive' video bytes are subject to virality.[57] Research also shows that when verified accounts put out hateful content, its virality is higher.[58] According to political scientist Neelanjan Sircar, "(w)ith social media and TV channels amplifying remarks and tweets even by minor politicians - many of whom find it the easiest way to make headlines - the hateful rhetoric seems 'pervasive' and 'non-stop'".[59] Frequent demands for content moderation often fail to garner sufficient response because social media platforms themselves profit from the spread of hate, as in the case of Facebook, according to revelations made by a whistleblower in 2021.[60]

The "Sulli Deals" and "Bulli Bai" incidents further demonstrate the role of social media and online platforms in dehumanising marginalized groups in India, especially women. The 'Sulli Deals' incident took place in July 2021 and was followed by a nearly identical incident, 'Bulli Bai', in January 2022.[61] In both these episodes, photographs and social media handles of more than a hundred Muslim women were put up for 'auction' on a Github application, whose users could then bid on the auctioned women.[62] After much furore, arrests were eventually made; however, all of the accused have been granted bail on 'humanitarian grounds' and as first time offenders.[63] Yet, "(f)emale journalists, human rights defenders, politicians and feminist activists" continue to be "particularly targeted [online] for physical and psychological violence and threats, including death",[64] with some even being arrested for their advocacy and denied bail.

The government's failure to protect against disinformation, hate speech, and online gender-based violence raises serious concerns around the protection of democratic digital space and basic civic freedoms.

---

57 Prerna Singh, "Populism, Nationalism, and Nationalist Populism," *Studies in Comparative International Development* 56, no. 2 (2021): 250–69, https://doi.org/10.1007/s12116-021-09337-6; see also Madeeha Fatima, Naomi Barton, and Alishan Jafri, "100+ Instances of Hate Speech, Religious Polarisation, Hindutva Supremacy in Adityanath's Poll Speeches," The Wire, accessed July 1, 2022, https://thewire.in/communalism/100-instances-of-hate-speech-religious-polarisation-hindutva-supremacy-in-adityanaths-poll-speeches.

58 Binny Mathew et al., "Analyzing the Hate and Counter Speech Accounts on Twitter" (arXiv, December 6, 2018), http://arxiv.org/abs/1812.02712.

59 Sharanya Hrishikesh, "Why People Get Away with Hate Speech in India," BBC News, April 13, 2022, https://www.bbc.com/news/world-asia-india-61090363.

60 Craig Timberg, "New Whistleblower Claims Facebook Allowed Hate, Illegal Activity to Go Unchecked," *Washington Post*, October 22, 2021, https://www.washingtonpost.com/technology/2021/10/22/facebook-new-whistleblower-complaint/.

61 "Bulli Bai: Sulli Deals 2.0? All You Need To Know About The Online 'Auction' Of Muslim Women," Outlook India, January 3, 2022, https://www.outlookindia.com/website/story/india-news-bulli-bai-sulli-deals-20-all-you-need-to-know-about-the-online-auction-of-muslim-women/408040.

62 "Bulli Bai: India App That Put Muslim Women up for Sale Is Shut," *BBC News*, January 3, 2022, sec. India, https://www.bbc.com/news/world-asia-india-59856619.

63 "Sulli Deals, Bulli Bai App Creators Granted Bail," *The Economic Times*, March 29, 2022, https://economictimes.indiatimes.com/tech/tech-bytes/sulli-deals-bulli-bai-app-creators-granted-bail/articleshow/90508973.cms.

64 Irene Khan, "A/HRC/50/29: Reinforcing Media Freedom and the Safety of Journalists in the Digital Age," Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (OHCHR), accessed June 24, 2022, https://www.ohchr.org/en/documents/thematic-reports/ahrc5029-reinforcing-media-freedom-and-safety-journalists-digital-age; see also Eliza Mackintosh and Swati Gupta, "Troll Armies, 'deepfake' Porn Videos and Violent Threats. How Twitter Became so Toxic for India's Women Politicians," CNN, accessed June 24, 2022, https://www.cnn.com/2020/01/22/india/india-women-politicians-trolling-amnesty-asequals-intl/index.html; "Safoora Zargar: Bail for Pregnant India Student Blamed for Delhi Riots," *BBC News*, June 23, 2020, sec. India, https://www.bbc.com/news/world-asia-india-53149967.

IV. Censorship: Crackdowns on Free Speech and Dissent

The increase in disinformation and harmful expression comes amidst the Government's increasing control over online space, which Access Now has termed "an epidemic of censorship and digital authoritarianism".[65] According to the Freedom on the Net Index, where India's scores have been consistently declining since 2018, excessive moderation of online content, the undermining of end-to-end encryption, increased website/application blocking, and a high volume of internet shutdowns are all limiting Indians' digital rights. Ironically, one example of the decreasing freedom on the Indian internet comes from the Government's order to Twitter to remove Freedom House's tweets discussing India's declining status in their Freedom in the World 2021 report.[66] India has also failed to join international coalitions working towards protecting human rights online, such as the Freedom Online Coalition and the U.S. Government's Declaration for the Future of the Internet.[67]

While those who violate the rights of marginalized groups are granted leniency, many journalists, human rights defenders, academicians, and political activists are currently languishing in jail, oftentimes for merely disagreeing with those in power, usually through simple tweets, speeches, or jokes expressed online. According to a Human Rights Watch report on the increasing criminalization of peaceful expression in India, the "government uses draconian laws such as the sedition provisions of the penal code, the criminal defamation law, and laws dealing with hate speech to silence dissent".[68]

Use of provisions related to sedition and other counterterrorism legislation such as the Unlawful Activities (Prevention) Act, 1967 to restrict dissent has increased exponentially since 2014. Article 14's study of sedition cases over the last decade reveals a 28% rise in such cases, in violation of Supreme Court guidelines, especially against critics and protesters since 2014.[69] In one instance, sedition charges were filed against climate activist Disha Ravi, for editing and sharing online a 'toolkit' document about the 2021

65 "The Indian Government's Torrent of Digital Censorship, Intimidation Must Stop," *Access Now*, June 10, 2021, https://www.accessnow.org/indian-government-digital-censorship-intimidation/.

66 "Govt Asks Twitter to 'take down' Freedom House's Tweets on Declining Internet Freedom in India: Entrackr," Newslaundry, June 27, 2022, https://www.newslaundry.com/2022/06/27/govt-asks-twitter-to-take-down-freedom-houses-tweets-on-declining-internet-freedom-in-india-entrackr; see also Freedom House [@freedomhouse], "(1/5) Freedom House Is Concerned That the Indian Government Ordered Twitter to Restrict Our Tweets Last Year.," Tweet, *Twitter*, June 30, 2022, https://twitter.com/freedomhouse/status/1542538616437673984.

67 "About Us," *Freedom Online Coalition* (blog), accessed June 24, 2022, https://freedomonlinecoalition.com/about-us/; see also "Declaration for the Future of the Internet," *United States Department of State*, accessed June 27, 2022, https://www.state.gov/declaration-for-the-future-of-the-internet/.

68 "Stifling Dissent: The Criminalization of Peaceful Expression in India" (Human Rights Watch, May 24, 2016), https://www.hrw.org/report/2016/05/25/stifling-dissent/criminalization-peaceful-expression-india.

69 "Our New Database Reveals Rise In Sedition Cases In The Modi Era — Article 14," accessed July 4, 2022, https://www.article-14.com/post/our-new-database-reveals-rise-in-sedition-cases-in-the-modi-era.

farmers' protests in the country.[70]

Recently, the Supreme Court put on hold all pending trials, appeals and proceedings related to sedition while examining a batch of petitions challenging the constitutional validity of the provision, until the Central Government completed its exercise in re-examining the provisions.[71] However, whether the use of the provision will actually cease remains to be seen. Previously, another provision which criminalised online speech, Section 66A of the Information Technology Act, 2000 (IT Act), was struck down by the Supreme Court.[72] Nonetheless, the use of the provision to restrict speech continues, with as many as 745 cases under the provision still pending as of March 2021.[73]

Other laws, including criminal code provisions on promoting enmity between communities, continue to be used to suppress online speech. In one such instance, Gujarat member of the legislative assembly (MLA) Jignesh Mevani was charged with criminal conspiracy and promoting enmity between communities under the Indian Penal Code, 1860 (IPC) for tweets in which he called the Prime Minister (PM) Modi a worshipper of Mahatma Gandhi's assassin and advised the PM to appeal for peace and harmony during his visit to communal violence sites in Gujarat.[74] Similar charges of promoting enmity and outraging religious beliefs were also brought against Delhi University Professor Ratan Lal, a Dalit and human rights activist, who tweeted a sarcastic comment about the 'shivling' (a representation of the Hindu god Shiva) allegedly found at

Other laws, including criminal code provisions on promoting enmity between communities, continue to be used to suppress online speech.

70 Jignasa Sinha, "Disha Ravi Toolkit Case: With Probe Making No Headway, Closure Report May Be an Option," *The Indian Express*, October 27, 2021, https://indianexpress.com/article/cities/delhi/disha-ravi-toolkit-case-with-probe-making-no-headway-closure-report-may-be-an-option-7590653/.

71 Bhadra Sinha, "In Historic Order, SC Suspends Sedition Law, 'hopes & Expects' Govts Will Stop Pursuing It," *The Print*, May 11, 2022, https://theprint.in/judiciary/in-historic-order-sc-suspends-sedition-law-hopes-expects-govts-will-stop-pursuing-it/951302/.

72 "Explained: The Shreya Singhal Case That Struck down Section 66A of IT Act," *The Indian Express*, July 17, 2021, https://indianexpress.com/article/explained/explained-the-shreya-singhal-case-that-struck-down-section-66a-of-it-act-7408366/.

73 Krishnadas Rajagopal, "'Distressing' and 'Shocking' That People Are Still Tried under Section 66A of IT Act, Says SC," *The Hindu*, July 5, 2021, sec. National, https://www.thehindu.com/news/national/distressing-and-shocking-that-people-are-still-tried-under-section-66a-of-it-act-says-sc/article35142975.ece; see also "Zombie Tracker" (Internet Freedom Foundation), accessed July 4, 2022, https://zombietracker.in/.

74 "Gujarat MLA Jignesh Mevani Arrested by Assam Police for Tweets on PM Modi," Text, Scroll.in (https://scroll.in), accessed July 4, 2022, https://scroll.in/latest/1022281/gujarat-mla-jignesh-mevani-arrested-by-assam-police.

the Gyanvapi mosque in Varanasi.[75]

In 2021, the Amazon Prime web series, 'Tandav', came under fire for its controversial portrayal of Lord Shiva, as a result of which multiple first information reports (FIRs, documents prepared by police after verifying a complaint) were filed for allegedly hurting religious sentiments of Hindus.[76] This controversy was further used by the Government to justify introducing the restrictive Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[77] Part III of the Rules relates to the regulation of digital news media and OTT platforms, such as Netflix, Amazon Prime and Disney+Hotstar, and essentially would create the equivalent of a 'heckler's veto' in India, allowing for censorship of legal speech if it is seen to offend certain groups.[78]

The rise in censorship of legitimate speech online, particularly sentiments critical of the government or ruling majority, while hate speech and disinformation targeting minorities spreads with impunity, continues to raise serious concerns regarding the protection of civic freedoms in India.

75 "Delhi Police Arrest DU Teacher Ratan Lal Over Social Media Post on Gyanvapi 'Shivling,'" The Wire, accessed July 4, 2022, https://thewire.in/rights/delhi-police-arrest-du-teacher-ratan-lal-over-social-media-post-on-gyanvapi-shivling.

76 "Bengaluru: FIR Filed against 'Tandav' Makers, Actors for Allegedly Hurting Religious Sentiments," Text, Scroll.in (https://scroll.in, January 24, 2021), https://scroll.in/latest/984984/bengaluru-fir-filed-against-tandav-makers-actors-for-allegedly-hurting-religious-sentiments.

77 Namrata Maheshwari, Ria Singh Sawhney, and Akhil Thomas, "How the Modi Government's New IT Rules Jeopardise the Right to Privacy and Free Speech," Text, Scroll.in (https://scroll.in, November 22, 2021), https://scroll.in/article/1010778/how-the-modi-governments-new-it-rules-jeopardise-the-right-to-privacy-and-free-speech.

78 "Tandav Is a Case Study for OTT Censorship under the IT Rules, 2021 #LetUsChill," Internet Freedom Foundation, March 27, 2021, https://internetfreedom.in/tandav-case-study/.

V. Conclusion

Increasing hate speech, curbs on dissent and overbroad surveillance have all contributed to the shrinking of online civic space in India. Attacks on human rights defenders, protesters, journalists, activists and their illegal surveillance further showcase the harm that infringements of digital rights are having on civil liberties and democratic ideals in India.

It is imperative to both document and address the harms caused by the misuse of technology by authoritarian actors. India and the international community must take steps to ensure that sufficient legal safeguards are enacted to protect against misuse stemming from abuse of digital technologies – and in particular, ensure the protection of civic freedoms for civil society and vulnerable communities.

Appendix

TABLE 1: INDIA'S PERFORMANCE ON WORLD HUMAN RIGHTS INDICES FROM 2018-22

NAME OF INDEX	RANK/SCORE IN 2018	RANK/SCORE IN 2019	RANK/SCORE IN 2020	RANK/SCORE IN 2021	RANK/SCORE IN 2022
Democracy Index	41	51	53	↓ 46	NA
Economic Freedom of the World Index	105	↓ 108	NA	NA	NA
Freedom in the World	77	↓ 75	↓ 71	↓ 67	↓ 66
Freedom on the Net Index	57	↓ 55	↓ 51	↓ 49	NA
Human Development Index	130	↓ 131	= 131	NA	NA
Human Freedom Index	111	↓ 119	NA	NA	NA
Index of Economic Freedom	130	129	120	↓ 121	↓ 131
Rule of Law Index	62	↓ 68	↓ 69	↓ 79	NA
Women Peace & Security Index	131	↓ 133	133	↓ 148	NA
World Press Freedom Index	138	↓ 140	↓ 142	= 142	↓ 150