The Unfreedom Monitor

A Methodology for Tracking Digital Authoritarianism Around the World

INDIA

COUNTRY REPORT

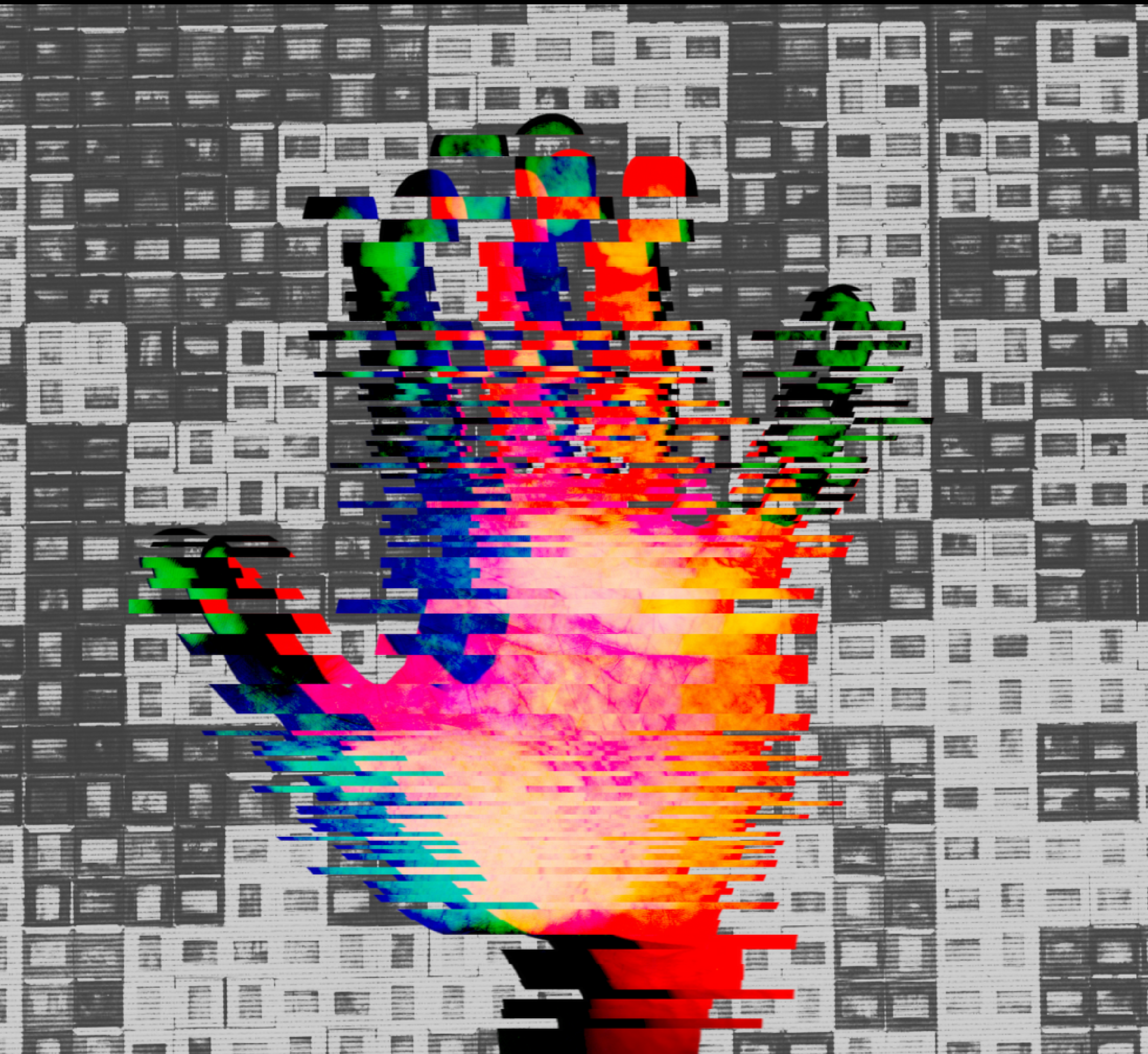

Table of Contents

Acknowledgements

The Unfreedom Monitor is the collective work of dozens of researchers and writers spread across multiple countries and working in time zones. Desk research was supported by colloquia and research assistance from the Global Voices community. In the interests of security, the names of all the team members have been withheld in this report. For citation purposes, the report can be attributed to "Global Voices Advox." Any errors or omissions should also be addressed to Advox at **advox@globalvoices.org**. Funding for this project was provided by the Deutsche Welle Academy (DW) which in turn received funding from the Federal Republic of Germany through the BMZ, as well as by other Global Voices supporters, a list of which can be found on our sponsors page.

Stichting Global Voices
Kingsfordweg 151
1043GR Amsterdam
The Netherlands
https://globalvoices.org

EXECUTIVE SUMMARY

This report aims to analyse the key motives for, methods of, and responses to digital authoritarianism in India. As the world's largest democracy, the elected government plays a critical role in protecting citizens from threats and imparts duties under its mandate of being a welfare state. However, this report finds that these same narratives are used to justify a vast range of digital authoritarian practices that end up curtailing citizens' digital liberties. Surveillance and censorship are carried out for national security, law and order, and public safety reasons. A tweet supporting the farmer's protests online becomes a "threat" that needs to be taken down and a rally against the government's policies becomes a "threat'' warranting an internet shutdown. The Indian state's frequent attempts to censor content, both online and offline, that it believes is against a norm or value is a manifestation of the same phenomenon. For instance, an "anti-national'' post is a threat against India that calls for censorship.

In addition to protection against threats, the well-intentioned "e-welfare state'' that aims to ease citizens' lives ends up infringing digital liberties. Technology is rapidly being used for governance and *to govern*. In this vein, the digital public sphere in the country is almost a well-curated sphere where there is enough data on everyone and a strong grip over who and what is accepted. Digital IDs, mobile apps, and centralised databases bring with them issues of exclusion, surveillance, and infringement of privacy.

India uses many methods to curtail digital rights and liberties across the themes of data governance, speech, access, and information. Together, they mirror a system where citizens' moves are surveilled and speech curtailed. At the same time, there is strong pushback against these practices. Digital authoritarian practices are widely reported, scrutinised, and questioned by civil society members, media, the judicial system, and political leaders, creating a system of checks and balances.

BACKGROUND

Country Challenge

In 2021, celebrating the sixth anniversary of the Digital India Mission, Prime Minister Narendra Modi declared that the next decade would be India's "Techade'"(The Hindu). At another event, he spoke about how the digital age has "refined" all aspects of politics, economy, and society. He adds that technology and data have become the "new weapons" in a changing world order ("In digital age, technology and data are new weapons, says PM Modi"). Indeed, the digital has become an integral part of governance and society in the country. The government has embraced the digital economy, digital infrastructures, and e-governance. In a global pandemic, in addition to on-ground healthcare, the country relied on technological tools such as mobile apps, drones, and telecom data. Social media has been an important platform for public discourse within the country and the general elections 2019 were colloquially referred to as the country's "WhatsApp elections." At the same time, embracing the digital has come with ramifications for politics, public life, civic discourse, and society at large. Adopting a digital economy comes with burning questions of who reaps the benefits, particularly in a country with deep inequalities (Gurumurthy et al.).

The country's digital ID system Aadhaar[1] raises concerns about exclusion (Ramanathan) with people losing their lives as the system failed to recognise them (Bhardwaj). The government wants to make India a "global drone hub" by 2030 ("India to become global drone hub by 2030, Says Jyotiraditya Scindia"); simultaneously, drones monitor protestors, curbing their freedom of expression. During the pandemic, the country became a locus of misinformation and disinformation with "CoronaJihad" trending on Twitter (Bajoria). While social media is becoming a medium for political discourse, political parties have weaponised it for their gain. In general, despite the platforms' promises of creating a safe space and connected world, social media has become an unsafe space for religious minorities, women, Dalits, and other marginalised groups. In some instances, violence online has translated to offline violence and even led to the loss of lives (Kain et al. 7).

Moreover, the country does not have a robust legal infrastructure underpinning many of these technologies, or a dedicated data protection legislation, which limits the avenues for citizens to seek recourse.

COUNTRY POLITICAL HISTORY

Overview of the country's political system, major events, and press freedom

India is a sovereign, secular republic and follows a parliamentary system of government. ("Governance & Administration''). The country's constitution confers certain powers to the Union and state governments, and lays down a clear separation of powers between the executive, judiciary, and legislature ("THE CONSTITUTION OF INDIA"). The country periodically conducts elections overseen by the Election Commission, an autonomous, constitutionally backed body. At the national level, there are broadly two major parties: the Indian National Congress (INC) and the Bharatiya Janata Party (BJP). Several regional political parties contribute to the diverse political system. The INC led India's freedom struggle and remained in power for the vast majority of the country's political history, until 2014. Towards the end of its tenure, the party was criticised for its stagnant growth and corruption paving way for the BJP, a right-wing party supporting the idea of Hindu nationalism.

Under the leadership of Prime Minister Narendra Modi, the BJP has won a popular mandate for two terms now. While those who support the prime minister and the party view him as a strong able leader that takes swift action, those who oppose him worry about the decline in democratic and secular values. For example, in 2016, by simply announcing it at a press conference, the government of India demonetised all 500 and 1000 rupee notes as a move to fight corruption, and reduce black money and terror funding (Ministry of Finance, Press Information Bureau). Critics argue that this was a unilateral executive decision taken without considering the disproportionate impact on the country's vast majority who rely on cash. (Ghosh et al.). With a majority in the lower house of parliament, the government has passed various legislations that have been met with criticism. One of the most prominent decisions taken in recent history is the abrogation of Article 370 of the Constitution that gave special status to Jammu Kashmir. The move and the way it was carried out was heavily criticised

[1] Aadhaar is a 12 digital unique ID provided to all residents in the country.

by opposition leaders, journalists, and civil society groups. In the days leading up to the decision and after, a complete internet shutdown was imposed, communication restricted, local leaders detained, and journalists gagged in the region. Besides Kashmir, there have also been protests against contentious legislations such as the Citizenship Amendment Act (CAA) and farm reforms leading to large scale protests.

Over the last seven years, civil society members and academics have expressed concern about the decline in the country's democratic values and freedom of expression, and the increased atmosphere of intolerance towards religious minorities facilitated by statements made by those in power (Gill). Civil society groups have repeatedly found themselves under pressure from the government: the cancellation of foreign funding, the use of repressive legislation, the shutting down of offices, including that of Amnesty International, legal charges, and raids are some of the methods used (Roth). In addition, dissenters and the media continue to operate in an atmosphere of fear with draconian anti-terror and sedition laws used against them (Roth).

The technological developments discussed in this report must be viewed in this larger socio-political context.

Press freedom

The country has many newspapers, broadcast channels, online publications, and radio channels in various regional languages besides Hindi and English. As of March 31, 2021, 1,44,520 newspapers and other periodicals are registered. (Registrar of Newspapers in India). Broadcast media is thriving, with 392 news channels operational. (Krishnan). However, there are some challenges to the free press in the country, ranging from press ownership, media bias, and government interference, to sensational coverage, paid news, and fake news (Krishnan). Media ownership is concentrated in a few hands, which is coupled with the fact that the majority of the media companies in the country have some business or political ties ("Media ownership monitor India"). Media critical of the government are penalised through various measures such as tax raids and reduced allocation of television licences, and are labelled "anti-national" (Repucci). The Editor's Guild of India has issued multiple statements condemning the arrests, intimidation and harassment of journalists, including the use of sedition and anti-terror laws (Editor's Guild of India). In 2020, "Modi's Yoddas" made it to Reporters Without Borders' list of global digital predators that stifle press freedom ("RSF unveils 20/2020 list of press freedom's digital predators"). During the COVID-19 pandemic, journalists publishing stories critical of the government were arrested, stifling press freedom. Additionally, there has been a systematic assault on Kashmiri media and local press since 2019 (Chakravarty). Certain new legislations threaten press freedom creating an ecosystem where the press cannot function freely. For instance, under the Information Technology (Intermediary guidelines and digital media ethics codes) Rules 2021, digital media outlets and over-the-top platforms are subjected to government oversight.

Overview of the country's internet pattern and penetration

India's public accessed internet services for the first time on August 15, 1995, and, as of September 2021, there are 834.29 million internet subscribers (Telecom Regulatory Authority of India 2). Out of this, 809.82 million are wireless internet subscribers, and only 24.47 million are wired internet subscribers (Telecom Regulatory Authority of India). Additionally, a rural-urban divide and a digital gender divide limit meaningful access (Telecom Regulatory Authority of India). Only 33.3 percent of women between the ages of 15 and 49 have ever used the internet (Paul and Bhushan 3). Out of this percentage, 51.8 percent belong to an urban setting (Paul and Bhushan 3). The government has taken several initiatives to improve connectivity, infrastructure, and access, however, policy gaps hinder progress (Internet Freedom Foundation). Besides this, social media is a popular medium in the country. WhatsApp continues to be the most popular social media site, with 530 million users, followed by YouTube with 448 million users, and Facebook with 410 million users (Ministry of Electronics & IT, Press Information Bureau). There are 210 million Instagram users in India and 17.5 million Twitter users (Ministry of Electronics & IT, Press Information Bureau). Apps such as Signal and Telegram are gaining popularity, and the micro-blogging site Koo is also gaining momentum (Inamdar).

METHODOLOGY

The report combines the analysis from the Civic Media Observatory (CMO) and desk research to map the different ways in which the government has used technology to expand its power in a manner that could potentially impact human rights negatively across the four themes: (i) data governance (ii) access (iii) speech (iv) information.

One limitation of the research is that media items for the CMO are only in English.

MOTIVES

This section will look at the narratives and justifications given by authorities for digital authoritarian practices in the country. It will also evaluate some key events that trigger such patterns and factors influencing the narratives.

The study finds that the Indian state uses three broad narratives to advance technological measures and take decisions that infringe digital liberties: 1) it protects citizens against some form of threat, 2) it eases citizen's lives and benefits them, 3) it is necessary for compliance with Indian laws.

PROTECT CITIZENS AGAINST THREATS

India uses the narrative of protecting its citizens and society from some form of threat (real or perceived) to justify authoritarian practices. Given that the state has a reasonable mandate to protect its citizens and enforce rights, this narrative is built into the Indian Constitution and legal framework. For instance, Article 19 of the Constitution guarantees the fundamental right to expression subject to reasonable restrictions.[2] However, as pointed out by legal experts, these terms are broad and vague subject to misuse: a trend that is recurrent across the use of various technologies.

National security

National security is a ground for expanding surveillance (Shekar and Mehta), putting limitations on privacy, imposing censorship, and restricting access to information. Research on the mass surveillance programs instituted by the government shows that the majority of the surveillance systems were conceptualised in the aftermath of the 2008 terror attacks (Xynou). Similar narratives are used to justify the expansion of technologies such as CCTV, drones, and facial recognition technology (FRT). For instance, in an RTI response, Delhi Police justified the use of FRT during republic day celebrations to avoid any mishap based on security threats from militant groups ("RTI to Delhi Police on Facial Recognition"). Discussing the case of Hyderabad, one of the most surveilled cities in the world, Srinivas Kodali, an independent researcher, points out how surveillance culture in the state was triggered in the aftermath of the twin bombings that took place in the city in 2007.

In addition to surveillance, though limited, national security is also used to justify the blocking of access to content online and placing restrictions on press freedom. Through 2020 and 2021, the Indian government blocked several Chinese apps due to national security reasons (Bhowmik et al.). In 2022, Media One, a Malayalam news channel critical of the government, was blocked by the Ministry of Information and Technology citing national security and public order considerations (Ministry of Information and Broadcasting, Press Information Bureau).

[2] These include: a) interests of the sovereignty and integrity of India b) the security of the State c) friendly relations with foreign States d) public order, decency or morality e) relation to contempt of court f) defamation or incitement to an offence.

Public order, law and order, public safety, crime prevention

Maintaining public order, law and order, and ensuring public safety are among the most common reasons the state gives for expanding surveillance and censorship of speech. Cities are loaded with CCTV cameras to prevent crime and enhance women's safety. There is rich literature on speech restrictions on the pretext of "public order" (Bhatia) (Acharya 159). Technological tools such as social media monitoring, takedown requests, and internet shutdowns are the only enablers of this phenomenon. One of the most recurrent reasons authorities impose an internet shutdown is to prevent offline harm during law and order situations ("Living in Digital Darkness"). Law enforcement agencies also routinely have justified tracking social media to maintain law and order (Parashar).

Fake news, disinformation, and misinformation

> *Curbing fake news, misinformation, and disinformation is used as a narrative to bring in laws to regulate online spaces, block websites, monitor speech online, enforce internet shutdowns, and restrict the press.*

While issues of misinformation and disinformation are very real and multi-dimensional issues in the Indian context (Goel), they are sometimes misused to curb digital liberties. Political parties have profited from spreading misinformation and disinformation polarising communities, especially during political events and elections ("The Wire: Heartland Hatewatch"). At the same time, curbing fake news, misinformation, and disinformation is used as a narrative to bring in laws to regulate online spaces, block websites, monitor speech online, enforce internet shutdowns, and restrict the press. In a study by the Centre for Internet and Society exploring the threats to digital expression online by the Union government, the authors note how governments had suppressed critical journalistic reporting under the pretext of curbing misinformation during COVID-19 (Manogna et al.) Similarly, during the protests against the controversial Citizenship Amendment Act (CAA), law enforcement in various cities arrested people for their social media posts under the pretext of curbing fake news ("Anti-CAA protest: Police monitoring some social media handles to check spread of misinformation"). In February 2022, the Ministry of Information and Broadcasting blocked 35 YouTube channels, two websites, and a few social media accounts for "spreading coordinated anti-India disinformation over the internet and 'anti-India fake news' about sensitive political issues" (Ministry of Information and Broadcasting, Press Information Bureau).

It is important to note that while the sensitivity of the issues and power of social media might warrant state intervention, each case needs to be evaluated in the larger socio-political climate of the country.

Additionally, laws that are passed with the intention to curb fake news end up undermining press freedom and digital liberties. Two such instances are the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (Press Information Bureau) and the new Media Policy in Kashmir ("Media Policy 2020").

Anti-national speech and action

Speech is restricted for being "anti-national," though the word is not defined in any Indian statute. In 2021, the police in the state of Uttarakhand declared that those posting anti-national content on social media might be denied passports and arms licences (Das). In February 2022, police arrested a Kashmiri journalist for posting content that was "anti national" and "with a criminal intent to disturb the law and order" ("Kashmir journalist arrested for 'anti-national' content on social media").

Harm against societal values or norms

On various occasions, the government has restricted speech when it believes there is a threat to a norm and value it views as sacrosanct. Topics such as religion, Indian values, nationalism, and the armed forces are usually hotbeds for charges of sedition, defamation, and censorship, depending on the perceived harm (Kovacs and Ranganathan).

EASING CITIZEN'S LIVES THROUGH DIGITALISATION, TECHNO-SOLUTIONS AND GOOD GOVERNANCE

Researchers and scholars have argued that surveillance and the centralisation of data are normalised under "digitalisation," "techno-solutionism," and "e-governance" (Ramanathan). They argue that Aadhaar, National Health ID, and Aarogya Setu were all introduced as a mechanism to ease citizens' lives but could potentially be used to surveil and infringe on privacy. In the same vein, challenging the notion of e-governance, civil society groups are concerned about the privacy infringement of the new centralised database Agristack that stores various data points of millions of farmers. Similarly, initiatives that gather a wide range of data, such as the National Media Analytics Centre (NMAC), a software that tracks conversations online and classifies comments, were introduced with the aim of "better governance" and "gauging public opinion" (Sinha).

COMPLIANCE WITH INDIAN LAW

On various occasions, the Indian state has asked social media companies to take down posts and adopt certain rules, in order to comply with Indian laws. While the law of the land allows for this, it is important to note that it is used as a way to exert power. Non-compliance by social media giants also invites legal action and intimidation. For instance, in February 2021, the government threatened legal action against Twitter when it did not initially comply with the orders to remove tweets concerning the farmer's protests (Bhargava). In another case that year, the government sent legal notices to Twitter, citing sections from the Information Technology Act 2000, to take down tweets that it claimed were spreading fake news related to COVID-19 (Deep). Critics of the move believed this was an act of censorship and a means to curb information that was critical of the government's handling of COVID-19 ("India Covid: Anger as Twitter ordered to remove critical virus posts").

EVENTS THAT HAVE TRIGGERED AN EXPANSION OF DIGITAL AUTHORITARIANISM

This section will look at some of the events where the state has infringed on citizens' digital liberties, paving a path for digital authoritarianism that may outlive the event itself. In general, events that have led to disruption in day-to-day affairs (such as protests) requiring more significant state intervention are ripe for digital authoritarianism:

Terror attacks, security threats

As noted in the previous section, research has pointed out the apparent expansion of state power in the aftermath of the 2008 terror attacks in the country.

Protests

During protests, authorities use various technological measures such as drones, CCTV, and facial recognition, to surveil citizens (Advox). Additionally, as protestors take to social media, these spaces are monitored and censored (Twitter). The government also shuts down the internet and blocks certain types of communication. This has been a common thread across the recent protests that have taken place against the Citizenship Amendment Act 2019, farm reforms 2020, and the abrogation of Article 370.

> *Using inputs from former and present employees of Facebook, a Wall Street Journal article alleged that Facebook did not take action against online hate speech by the ruling party, fearing that it might harm business prospects*

Elections

Countries worldwide have witnessed how powerful entities use social media and the mainstream media for their vested interest, and India is no exception to this (Rao). News reports allege that political parties in India have used the services of Cambridge Analytica (Aneja). There is also the problem of increased hate speech, particularly against minorities, during elections by those in power. Allegations of bias and selective intervention by social media companies such as Facebook compound the problem. Using inputs from former and present employees of Facebook, a Wall Street Journal article alleged that Facebook did not take action against online hate speech by the ruling party, fearing that it might harm business prospects (Punell and Horwitz). Further, the report claimed that BJP had received favourable treatment from Facebook during the 2019 elections (Punell and Horwitz).

Major political events

Major political events, such as the abrogation of the Article 370, protests, elections, and military action provide fertile conditions for the expansion of digital authoritarianism. In a politically charged atmosphere, disinformation and misinformation are also prevalent, both online and offline (Campbell-Smith and Bradshaw 5). As noted previously, censorship under the pretext of curbing fake news and misinformation is a concern, especially during political events. Other forms of repression, such as internet shutdowns and social media censorship, are recurring phenomena during such times. Mainstream media also contribute to the noise by airing sensationalised content supporting the governmental agenda in some instances.

COVID-19

COVID-19 saw an expansion of state power and the use of multiple technological initiatives that experts worry could outlast the pandemic. Numerous mobile apps, drones, portals, AI tools, and telecom data were used to enforce lockdown (Vijayakumar, and Ranjit). Privacy experts were concerned about the massive quantities of personal data collected without safeguards by the contact tracing app Aarogya Setu. In 2021, an RTI revealed that the app's data was shared with law enforcement in a district in Jammu and Kashmir, raising more apprehensions (Bhatnagar). In addition to this, there were multiple instances of censoring speech critical of the government during the pandemic.

JUSTIFICATIONS FOR DIGITAL AUTHORITARIAN PRACTICES

This section will look at the extent and nature of justification the government uses when advancing digital authoritarian practices in the country. Digital authoritarian practices in the country are complex and multidimensional phenomena with multiple stakeholders, such as the government, law enforcement, private players, and foreign corporations, each playing a distinct role. The previous section has shown that this expansion is not always evident and unidirectional. In a democracy, there is a mandate for transparency and accountability in the government's work bringing digital authoritarian practices to light. Through discussion in parliament, scrutiny by the opposition, civil society groups, and judiciary, the powers of the legislature and executive are kept in check. At the same time, there are some limitations:

Lack of legislative backing

Many of the country's key technological interventions, including those that amass a wide range of data, function without robust legislative backing — a common criticism flagged by several civil society groups and privacy advocates. These include mass surveillance programs such as the National Intelligence Grid (NATGRID) and Centralised Monitoring System (CMS), facial recognition systems, and Aarogya Setu, to name a few.

Inadequate discussion in parliament

Though laws are passed in parliament, there is limited discussion in certain cases. Significant amendments to the IT Act 2000 were passed hurriedly without debate (Pahwa). In 2016, the government introduced the overarching legislation governing Aadhaar as a money bill that limited the scope for scrutiny by the Upper House of the Indian Parliament (Bhatia). In other cases, there is no little to no discussion of the uses or dangers of certain technologies such as facial recognition despite their massive growth and use by law enforcement (Hickok).

Executive overreach

In the absence of legislative backing, many of these technological tools are backed by executive orders. For instance, In 2009, the birth of Aadhaar was by an executive notification rather than legislation. Besides this, a number of tech tools are governed by the rules framed by the executive under a parent legislation. For example, the recently passed IT Rules 2021, described as the "largest expansion of government control over speech in the country in the last decade" (Pahwa) was primarily an executive decision ("Indian Authorities Tighten Control Over Online Content"). Internet shutdowns and drones in the country are also governed by rules rather than acts of parliament.

Limitations to India's pre-consultative process

Civil society organisations play an important role in scrutinising legislation and contributing to law-making through a pre-consultative process. While draft rules and bills are put out for scrutiny and comments, this has not been consistent. Civil society groups have pointed out that, in certain cases, government departments do not put the bills out for the stipulated 30 day period ("SFLC.in raises concerns with reticent stakeholder consultation by the National Health Authority").

Information denied through the Right to Information Act

Seeking information using the Right to Information (RTI) Act is another powerful way for civil society organisations and the public at large to gain insight into governmental functioning. It has resulted in some critical revelations, though, in many cases, information is either not provided within the stipulated period (and, when provided, responses are evasive), or simply denied citing national security reasons.

Role of foreign governments and corporations

Digital authoritarian practices in India are also influenced by foreign governments and companies. For instance, surveillance infrastructure in terms of CCTV and drones are also provided by foreign companies. Having said that, as India is a sovereign republic, the government plays a critical role in enabling any use or misuse of technology. In certain cases, it has pushed back as well. It is noteworthy that while China is considered to be one of the key players in the export of surveillance technologies globally, there have been a few policy decisions undertaken by the Union Government that signal a shift in India's use of Chinese based surveillance technology (Chikermane). In May 2021, the Indian government excluded ZTE and Huawei from participating in the 5G trials in the country. Chinese drones were an important part of India's upcoming drone ecosystem; however, the government's recent decision to ban imports of drones is likely to change that dynamic (Chikermane).

Additionally, as discussed earlier, social media companies such as Facebook and Twitter have proven to influence public discourse. This will be discussed more in the next section.

METHODS

This section will discuss the key technology tools used to enable digital authoritarianism in the country across the themes of data governance, speech, access, and information. Many of these technologies are operationalised through public-private partnerships.

TECHNOLOGICAL TOOLS

Data Governance

Mass surveillance programs
India has as many centralised systems that amass, intercept, and monitor large amounts of data, and substantial budgetary allocations have been made to many of them. Most of these programs are run with opacity and no oversight and are closed to investigation due to national security reasons. Analysing these programs, technology policy expert Udhbav Tiwari points out that the available public information about mass surveillance systems has dwindled since 2014.

Spyware and intrusive technology
From time to time, investigative reports have shown that India has allegedly imported spyware and used it on human rights defenders:

- FinFisher: In 2013, an investigative report by the Citizen Lab revealed that it found command and control servers of an intrusive monitoring software FinFisher in India (Marquis-Boire).

- Netwire: Citizen Lab Toronto and Amnesty International claim that at least nine human rights defenders in the country were targeted with spyware called Netwire between January and October 2019 (“India: Human Rights Defenders Targeted by a Coordinated Spyware Operation”).

- Pegasus: There have been allegations of the government importing the spyware as part of a USD two billion defence deal with Israel (Kaushik), and using it on opposition members, political figures, bureaucrats, journalists, editors of newspapers critical of the government, human rights defenders, academics, cabinet ministers, members of the judiciary, and potentially a sitting judge (Vardarajan). The matter is currently being investigated by a technical committee that was formed by the Supreme Court.

In addition to imported spyware, research indicates that India houses many foreign surveillance companies. Maria Xynou notes that in addition to some of the “most notorious” surveillance companies in the country, many Indian companies sell intrusive surveillance tools globally. While Xynou made her observations in 2014, as recently as 2020 Citizen Lab found links between Dark Basin, a hack-for-hire group, to the Indian company BellTroX InfoTech Service (Scott et al. 7).

Video-based surveillance (CCTV cameras, drones) including FRT

The use of CCTV camera footage, drones, and facial recognition is rapidly increasing in the country. According to a list published by Forbes in 2021, Delhi tops the charts in being the most surveilled city in the world with 1,826.6 CCTV cameras per square mile (Forbes India). Additionally, there is a massive push toward facial recognition tools, despite the absence of legislative backing. Data compiled by the digital rights organisation Internet Freedom Foundation (IFF) shows that there are at least 97 facial recognition systems in the country as of March 2022. The country is also building a National Automated Facial Recognition System. These developments come against the backdrop of law enforcement using drones, CCTV camera footage and FRT to monitor and surveil citizens.

Digital IDs

A rich literature exists on concerns of privacy, surveillance, and the exclusionary potential of India's digital ID system Aadhaar (Khera). Critics have pointed out that Aadhaar has been pushed at all levels of governance, making it mandatory in practice. Despite these concerns, there have been other proposals to create more IDs. In 2020, the government launched the National Digital Mission (renamed the Ayushman Bharat Digital Mission) under which various players in the health ecosystem, including citizens, will be given a health ID. Researchers point out how this ID has similar flaws to Aadhaar: a push to make it mandatory, concerns about a lack of privacy, and corporate interests (Kodali). In February 2022, the government mooted creating a "federated digital ID" that could replace all other IDs.

> *"According to a list published by Forbes in 2021, Delhi tops the charts in being the most surveilled city in the world with 1,826.6 CCTV cameras per square mile"*

Centralised databases

Privacy and data governance researchers have also expressed concerns about the creation of databases for multiple purposes ranging from the legal sector to the agricultural sector (Kodali).

Artificial Intelligence

There is a growing AI ecosystem in the country and a strong political will to further expand it (Marda). AI software and tools are also used by law enforcement in the country for predictive data analysis, making it a potentially important area for evaluating concerns of digital authoritarianism.

Speech

Blocking content online

Blocking content online is a prominent method used to curtail free speech and access in the country. While the government and court orders block thousands of websites, the process is opaque because orders are not publicly available. Civil society groups and independent researchers have published leaked lists and filed RTI requests to ascertain the scale of blocking. An RTI filed by Delhi based digital rights group Software Freedom Law Centre (SFLC) revealed that, between 2010 and 2018, 14,221 websites/URLs were blocked

(Marda). Additionally, an investigative report by Citizen Lab showed that India uses internet filtering as a mechanism to block content online. The report showed that URLs related to the Rohingya crisis, including coverage by news platforms such as Aljazeera and the Telegraph, were blocked. Another study shows that the different internet service providers in the country use various methods to block content, contributing to the culture of opacity (Singh et al.). Additionally, there has been a significant increase in the number of social media accounts blocked in recent years, from 471 in 2014 to 9,849 in 2020 (Arnimesh).

Take down requests (including social media)

The Indian state censors speech online by directing social media and big tech companies to take down content. According to a report by Comparitech in 2019, the government sent the most number of content take down requests to social media companies globally. Google's transparency report 2021 shows the Indian government sent the second highest content take down requests worldwide (Ahaskar).

In many cases, the content that is flagged for taking down is critical of the government or against a belief the government views as a threat (such as porn, or satire on religion). For instance, in May 2021, at the peak of India's deadly second wave, the government directed social media platforms to remove posts critical of the government's handling of the COVID-19 crisis ("Twitter, FB and others remove nearly 100 posts after govt order"). Similar requests were made during the protests against the Citizenship Amendment Act and farm reforms.

Monitoring content online (including social media)

Proposals to monitor the internet, including social media, have been deliberated since 2011 (Crook). Over the past few years, the government has repeatedly attempted to bring in a policy for tracking public opinion and social media online (Barik). In 2018, the government issued a notification for creating a "social media monitoring hub" that was withdrawn after the Supreme Court intervened (Venugopal). In 2020, amidst the pandemic, another tender was floated to create a similar system of monitoring social media online. Studying social media monitoring systems in the country, Amber Sinha notes that there are at least five different schemes and programs introduced by the government and law enforcement that conduct some form of social media monitoring in varying capacities and intents.

Access

Service disruptions

India is popularly called the world's internet shutdown capital, and there has been an upward trend in the number of shutdowns imposed, based on data analysed between January 2012 and April 2018 by SFLC. Between 2019 and 2021, the erstwhile state of Jammu and Kashmir has experienced one of the longest internet shutdowns in a democratic country, severely curtailing the region's fundamental rights. Partial disruption of service and internet shutdowns are imposed for a range of reasons from curbing protests to prevent cheating on examinations. These measures have a huge economic and political cost. In 2021, the internet was blacked out for a total of 317.5 hours and bandwidth was throttled for 840 hours, costing the economy USD 582.8 million (Woodhams and Migliano).

Information

Coordinated inauthentic behaviour

Coordinated inauthentic behaviour is a prevalent and complicated problem in the country. Evidence suggests that major national parties like the INC and the BJP have engaged in this behaviour (Gleicher). In April 2019, a month before the country's national elections, Facebook removed 687 pages and accounts engaged in coordinated inauthentic behaviour linked to the IT cell of the INC (Gleicher). In January 2022, based on a two-year-long investigation, The Wire alleged that the BJP had used a mobile app called "Tek Fog" to "artificially inflate the popularity of the party, harass its critics and manipulate public perceptions at scale across major social media platforms (Kaul and Kumar). In parliament, the government stated that it had taken note of the media report but could not find such an app on any of the prominent app and APK stores. However, the issue of coordinated inauthentic behaviour in the country is further complicated by foreign relations and politics. For example, A report from Stanford's Internet Observatory documented a mass coordinated inauthentic behaviour operating out of Pakistan posted polarising accounts on India-Pakistan relations and politics in India (Grossman et al.).

Influence campaigns

Research indicates that major political parties use a wide range of tactics to influence and persuade the public, such as private firms for data analytics, targeted advertisements, IT cells, and automation to create a false sense of popularity (Campbell-Smith and Bradshaw 3). The challenge is that these tactics contribute to misinformation and disinformation leading to the suppression of fundamental rights (Campbell-Smith and Bradshaw 3). Additionally, the issue of misinformation, disinformation and fake news in the country is compounded by selective action and allegations of political bias by major social media giants, as discussed previously in this report.

> *The ruling BJP party's troll armies, consisting of human volunteers and bots, have harassed and intimidated women, minorities, dissenters, and other groups online curbing their freedom of speech*

In addition to this, the country faces a unique challenge with troll armies. The ruling BJP party's troll armies, consisting of human volunteers and bots have harassed and intimidated women, minorities, dissenters, and other groups online curbing their freedom of speech (Chaturvedi).

Legislation

In addition to technological tools, different legislations allow for the expansion of digital authoritarianism in the country. Besides this, in some cases, new legislation is brought to further state interests.

Shortcomings of existing laws

One common criticism of many of the key laws governing the internet and communications is the use of broad and vaguely defined terms that allow governments to interpret it widely. The upcoming draft Personal Data Protection Bill 2019 also follows this trend, allowing the government to exempt itself from the provisions of the bill on broad grounds.

In those cases where safeguards are present, the rules that outline procedures for the government fall short. For instance, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017, that govern internet shutdowns, provide for a review committee to evaluate the legality of the shutdown orders. However, members of the committee are from the executive, limiting proper accountability (SFLC).

Use of laws beyond internet governance

There are laws beyond internet-specific legislation that are used to curtail speech online. Mapping the crimialisation of speech in India, feminist researchers and data governance experts Anja Kovacs and Nayantara Ranganathan argue that a host of laws in addition to the internet and communication governance, such as sedition, defamation, copyright law, and hate speech, are used routinely to criminalise free speech online (Kovacs and Ranganathan)

In some cases, the authorities pass broad policies that undermine speech and press freedom. For example, under Kashmir's social media policy, government employees are asked not to post any inappropriate or material harmful to the state, and are warned that their online movements would be observed by law enforcement (The government of Jammu and Kashmir).

New laws

At times, new policies and laws are formed to regulate spaces that are a threat to the government. For instance, scholar Arif Hussain Nadaf argues that as social media became more prevalent in Kashmir, authorities moved to regulate it. Similarly, observations are made about the IT Rules 2021 that cover digital media outlets and platforms like Netflix and Amazon — spaces seen as more liberal and safe from government control.

RESPONSES

Despite the declining media freedom, shrinking space for civic discourse, and atmosphere of fear, concerned citizens, parliamentarians, civil society groups, the media, the judiciary, and international organisations continue to challenge digital authoritarianism in a myriad of ways. In 2012, in response to the controversial Information Technology (Intermediaries Guidelines) Rules 2011, several resistance movements took place, including a citizen-led hunger strike. Civil society groups and media continue to hold the state accountable in various ways, from approaching courts to tracking government policies, maintaining data, and filing RTI requests. Aadhaar, the contact tracing app Aarogya Setu, the imposition of internet shutdowns, the mass state surveillance programs, and the facial recognition systems have been challenged in courts. In 2019, there were at least five different petitions filed in the Supreme Court against a controversial government notification that empowered ten agencies, under a section of the IT Act, to intercept communications. ("Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State"). In response to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, multiple media houses challenged the rules in various high courts. In many cases, the judiciary has been an important stakeholder in keeping check on arbitrary actions of the government. For instance, in 2015, in what is called a landmark judgement, the Supreme Court struck down a section of the IT Act that was vaguely worded allowing law enforcement and governments to misuse it. In another case, the Supreme Court's judgement in Anuradha Bhasin v Union of India, that challenged the internet shutdowns and restrictions on press freedom in Jammu and Kashmir, reaffirmed the vital role the internet plays in exercising core fundamental rights.

Media publications continue to report and carry out investigative journalism on digital authoritarian practices. For instance, the Wire, a digital media outlet slammed with defamation cases in the past, has continued its investigative work by reporting on Pegasus and Tek Fog. From time to time, certain government programs and initiatives have received attention from the international community. In 2013, Human Rights Watch warned that the mass surveillance program Central Monitoring system (CMS) could curtail digital liberties. ("India: New Monitoring System Threatens Rights"). The United Nation General Assembly's Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also took note of the CMS's potential to normalise unregulated surveillance without state accountability. More recently, in 2019, UN independent experts condemned the Union Government's series of communication blockades in the region of Jammu and Kashmir in the aftermath of the abrogation of Article 370 ("UN Rights Experts Urge India to End Communications Shutdown in Kashmir"). As part of its "Ban the scan" campaign, Amnesty International has partnered with the Internet Freedom Foundation, a digital rights group in India, and international human rights organisation ARTICLE 19 to halt the expansion of surveillance structures in Hyderabad. Additionally, in 2018, Edward Snowden called Aadhaar a "mass surveillance system that will lead to civil death for Indians" ("Aadhaar Is Mass Surveillance System, Will Lead to Civil Death for Indians: Edward Snowden"). In 2020, amidst the debate on Aarogya Setu's surveillance potential, an ethical hacker by the pseudonym of Elliot Alderson brought to the government's notice certain security vulnerabilities. ("Aarogya Setu App Responds to Hacker Elliot Alderson's Privacy Concerns; Says No Data at Risk").

ANALYSIS AND CONCLUSION

India's "techade" does show signs of digital authoritarianism that can potentially have far-reaching implications for politics, civil liberties and society. At the same time, these are not new challenges for the country. In the past, the Indian government has attempted to surveil, monitor, and censor citizens. Here, state power is like water that will fall through any cracks and holes in the system. The system will either flourish or get contaminated based on the nature of the water. This report shows how COVID-19, protests, and major political incidents provide a ripe avenue for expanding state power. The larger socio-political context, one filled with concerns about a decline in democratic values, secularism, and civil liberties, will determine the extent of harm, who gets harmed, and the ability to respond.

India's lack of solid legal frameworks governing key technologies allows authorities to further exert power. As seen in the case of Aadhaar, facial recognition systems, and Aarogya Setu, legislative backing is an afterthought. However, by then, significant damage is already done. Any adverse impact on digital and civil rights will be felt most by vulnerable groups and those critical of the government. Besides the lack of legal structures, as seen through the report, the law is also used to expand state power. Further, as analysed in this report, private players supplying surveillance technologies, and social media giants enable digital authoritarianism in the country.

Though gaps exist, digital authoritarianism is reported and challenged by media, civil society groups, courts, and concerned citizens. In many cases, this has proved to be extremely valuable, paving a way for a hopeful future.

SECTION VI: REFERENCES

"Aadhaar is mass surveillance system, will lead to civil death for Indians: Edward Snowden." *India Today*, 20 August 2018, www.indiatoday.in/technology/news/story/aadhaar-is-mass-surveillance-system-will-lead-to-civil-death-for-indians-edward-snowden-1319121-2018-08-20. Accessed 17 March 2022.

"Aarogya Setu app responds to hacker Elliot Alderson's privacy concerns; says no data at risk." *Business Today*, 6 May 2020, www.businesstoday.in/technology/news/story/aarogya-setu-app-responds-to-hacker-elliot-alderson-privacy-concerns-says-no-data-at-risk-257498-2020-05-06. Accessed 17 March 2022.

"Aarogya Setu data protocol norms issued". *The Hindu*. 12 May 2020, https://www.thehindu.com/news/national/aarogya-setu-data-protocol-norms-issued/article31560752.ece. Accessed 12 March 2022.

Advox. "Exploring the use of tech-based tools in India to curb dissent during protests". *Advox,Global Voices*, 2022, https://globalvoices.org/2022/04/01/exploring-the-use-of-tech-based-tools-in-india-to-curb-dissent-during-protests/. Accessed 18 April 2022.

Ahaskar, Abhijit. "India Ranks 2nd In Volumes of Content Takedown Requests by Govts, Google". *Techcircle*, 22 October 2021, https://www.techcircle.in/2021/10/22/india-ranks-2nd-in-volumes-of-content-takedown-requests-by-govts-google. Accessed 15 April 2022.

Aneja, Urvashi. "What Cambridge Analytica does is the norm, not an aberration." *Indian Express*. 23 March 2018. https://indianexpress.com/article/opinion/what-cambridge-analytica-does-is-the-norm-not-an-aberration-facebook-data-elections-5108518/. Accessed 10 April 2022.

"Anti-CAA protest: Police monitoring some social media handles to check spread of misinformation." *Times of India*, 18 December 2019, https://timesofindia.indiatimes.com/india/anti-caa-protest-police-monitoring-some-social-media-handles-to-check-spread-of-misinformation/articleshow/72872381.cms. Accessed 28 March 2022.

Arnimesh, Shanker. "Modi govt ordered blocking of 9,849 social media accounts in 2020, 2,000% more than 2014." *The Print*, 8 December 2021, https://theprint.in/india/modi-govt-ordered-blocking-of-9849-social-media-accounts-in-2020-2000-more-than-2014/778637/. Accessed 15 April 2022.

Bajoria, Jayshree. "Coronajihad Is Only the Latest Manifestation: Islamophobia in India Has Been Years in the Making". *Human Rights Watch*, 25 April 2020, https://www.hrw.org/news/2020/05/01/coronajihad-only-latest-manifestation-islamophobia-india-has-been-years-making.

Bergman, Ronen, and Mark Mazzetti. "The Battle for the World's Most Powerful Cyberweapon." *The New York Times*, 28 January 2022, www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.
Bhairav, Acharya. "Free speech in India: still plagued by pre-modern laws" Media Asia, vol 42:3-4, pp 157-160, DOI: 10.1080/01296612.2016.1150582

Bhardwaj, Mayank. "For India's poorest, Aadhaar can be the difference between life and death". *Live Mint*, 12 September 2018, https://www.livemint.com/Politics/5MSjgIb1a0Mq5Jooq1wu7O/For-Indias-poorest-Aadhaar-can-be-the-difference-between-l.html. Accessed 2 March 2022.

Bhargava, Yuthika. "Govt. Asks Twitter To Remove 1,178 Accounts". *The Hindu*, 8 February 2021, https://www.thehindu.com/news/national/govt-asks-twitter-to-remove-1178-accounts/article61753981.ece. Accessed 27 February 2022.

Bhatia, Gautam. "Free Speech and Public Order — The Centre for Internet and Society." *The Centre for Internet and Society*, 17 February 2016, https://cis-india.org/internet-governance/blog/free-speech-and-public-order-1. Accessed 28 March 2022.

Bhowmik, Sneha, et al. "India adds 54 more Chinese apps to ban list; Sea says it complies with laws." *Reuters*, 15 February 2022, https://www.reuters.com/world/india/sea-owned-game-free-fire-unavailable-india-after-ban-chinese-apps-2022-02-15/. Accessed 28 March 2022.

Campbell-Smith, Ualan, and Bradshaw, Samantha. "Global Cyber Troops Country Profile: India.", Oxford Internet Institute, University of Oxford, May 2019, demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-Profile.pdf.

Chakravarty, Ipsita. "Killing the story: How the Kashmiri press was silenced after the region lost autonomy". *Reuters Institute For The Study Of Journalism*, 2021, https://reutersinstitute.politics.ox.ac.uk/killing-story-how-kashmiri-press-was-silenced-after-region-lost-autonomy. Accessed 31 March 2022.

Chikermane, Gautam. "Excluding Huawei from India is part of a policy continuum." *ORF*, 7 May 2021, https://www.orfonline.org/expert-speak/excluding-huawei-from-india-is-part-of-a-policy-continuum/. Accessed 8 March 2022.

Crook, Jordan. "Indian Government Wants To Monitor Twitter And Facebook, Maybe Google And Skype Too." *TechCrunch*, 10 August 2011, https://techcrunch.com/2011/08/10/indian-government-wants-to-monitor-twitter-and-facebook-maybe-google-and-skype-too/. Accessed 16 April 2022.

Das, Kalyan. "Anti-National' Posts On Social Media? Uttarakhand Police Won't Verify Passport". *Hindustan Times*, 2 February 2021, https://www.hindustantimes.com/india-news/antinational-posts-on-social-media-uttarakhand-police-won-t-verify-passport-101612280497065.html. Accessed 21 February 2022.

Deep, Aroon. "Twitter Censors Tweets From MP, MLA, Editor Criticising Pandemic Handling". *Medianama*, 24 April 2021, https://www.medianama.com/2021/04/223-twitter-mp-minister-censor/. Accessed 15 April 2022.

"Forbes India - Delhi, Chennai among Most Surveilled in the World, ahead of Chinese Cities." *Forbes India*, 25 August 2021, www.forbesindia.com/article/news-by-numbers/delhi-chennai-among-most-surveilled-in-the-world-ahead-of-chinese-cities/69995/1.

"Finance Ministry: Demonetization immensely beneficial to Indian Economy and People." *Ministry of Finance, Press Information Bureau*, 30 August 2017, https://pib.gov.in/newsite/printrelease.aspx?relid=170378. Accessed 25 March 2022.

Ghosh, Jayati, et al. *Demonetisation Decoded A Critique of India's Currency Experiment*. 1st Edition ed., Routledge India, 2017.

Gill, Prabhjote. "India is ramping up the use of facial recognition to track down individuals without any laws to keep track of how this technology is being used", 10 February 2021 . *Business Insider India*.

Gleicher, Nathaniel. "Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan | Meta." *Meta*, 1 April 2019, https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/. Accessed 31 March 2022.

Goel, Kritika. "Here's Your Round-Up of All the Fake News Around CAA Protests." *The Quint*, 18 December 2019, https://www.thequint.com/news/webqoof/round-up-of-fake-news-around-caa-protests-students-police#read-more. Accessed 29 March 2022

Government of India. "Questions : Lok Sabha." *164.100.47.194*, Mar. 23AD, 164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=36180&lsno=17.

"Governance & Administration." *National Portal of India*, https://www.india.gov.in/topics/governance-administration. Accessed 25 March 2022.

"Government notifies Information Technology (IntermediaryGuidelines and Digital Media Ethics Code) Rules 2021" *Ministry of Electronics & IT, Press Information Bureau*. 25 February 2021. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749
https://www.businessinsider.in/tech/news/what-is-facial-recognition-technology-and-how-india-is-using-it-to-track-down-protestors-and-individuals/articleshow/80782606.cms

Grossman, Shelby, et al. “Reporting for Duty.” *Fsi.stanford.edu*, Stanford Internet Observatory, 1 October 2020, fsi.stanford.edu/news/reporting-duty.

“Guidelines For Accreditation Of Journalists Amended To Regulate Fake News.” Ministry of Information & Broadcasting, Press Information Bureau, 2 April 2018. https://pib.gov.in/newsite/PrintRelease.aspx?relid=178306

“Guidelines on the usage of social media by Government Employees”. *General Administration department, Government of Jammu and Kashmir*. 26 December 2017. https://www.kashmiruniversity.net/download/Social_Media_Policy.pdf

Gurumurthy, Anita et al. *Gender Equality In The Digital Economy: Emerging Issues, A New Social Contract For Women's Rights In The Data Economy*. Feminist Digital Justice, IT For Change, Bangalore, 2019, https://itforchange.net/sites/default/files/1620/Feminsit%20Digital%20Justice%20Issue%20Paper%201_%20updated%20name%20and%20logo.pdf. Accessed 18 March 2022.

Hickok, Elonnai et al. “Facial Recognition Technology In India”. *Centre for Internet and Society and The Human Rights, Big Data and Technology Project, University of Essex, UK*, 31 August 2021, https://cis-india.org/internet-governance/facial-recognition-technology-in-india.pdf.

“IFF releases the second edition of the Connectivity Tracker #MapTheDigitalDivide.” *Internet Freedom Foundation*, 14 January 2022, https://internetfreedom.in/iff-second-edition-connectivity-tracker/. Accessed 25 March 2022.

Inamdar, Nikhil. “Koo: India's Twitter alternative with global ambitions.” *BBC*, 4 February 2022, https://www.bbc.com/news/world-asia-india-60194920. Accessed 25 March 2022.

“Indian Authorities Tighten Control Over Online Content - Access Now”. *Access Now*, 2022, https://www.accessnow.org/indian-authorities-tighten-control-over-online-content/.

“India Covid: Anger As Twitter Ordered To Remove Critical Virus Posts”. *BBC News*, 2021, https://www.bbc.com/news/world-asia-56883483. Accessed 15 Apr 2022.

“In Digital Age, Technology And Data Are New Weapons, Says PM Modi”. *Business Standard*, 2021, https://www.business-standard.com/article/current-affairs/in-digital-age-technology-and-data-are-new-weapons-says-pm-modi-121111800239_1.htm.

“India: Human Rights Defenders Targeted By A Coordinated Spyware Operation”. *Amnesty International*, 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/.

“India strikes hard on Pakistani Fake News Factories Ministry of I&B blocks Pakistan funded fake news networks 35 YouTube channels, 2 websites blocked for spreading anti-India fake news.” *Ministry of Information and Broadcasting, Press Information Bureau*, 21 January 2022

“India: New Monitoring System Threatens Rights.” *Human Rights Watch*, 7 June 2013, www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.

“India to become global drone hub by 2030, Says Jyotiraditya Scindia”. *ANI News*, 26 August 2021, https://www.aninews.in/news/national/general-news/india-to-become-global-drone-hub-by-2030-says-jyotiraditya-scindia20210826171600/. Accessed 15 April 2022.

Kain, Damini et al. *Online Caste-Hate Speech: Pervasive Discrimination And Humiliation On Social Media.* CIS and APC, 2021, https://www.apc.org/en/pubs/online-caste-hate-speech-pervasive-discrimination-and-humiliation-social-media. Accessed 22 Mar 2022.

"Kashmir Journalist Arrested For 'Anti-National' Content On Social Media". *Mint*, 5 February 2022, https://www.livemint.com/news/india/kashmir-journalist-arrested-for-anti-national-content-on-social-media-11644027928240.html.

Kaul, Ayushman, and Devesh Kumar. "Tek Fog: An App with BJP Footprints for Cyber Troops to Automate Hate, Manipulate Trends." *The Wire*, 6 January 2022, thewire.in/tekfog/en/1.html. Accessed 18 February 2022.

Kaushik, Krishn. "India Bought Pegasus as Part of Defence Deal with Israel in 2017: NYT." *The Indian Express*, 30 January 2022, indianexpress.com/article/india/india-bought-pegasus-defence-deal-israel-2017-nyt-7746655/. Accessed 27 February 2022.

Khera, Reetika. Dissent on Aadhaar: Big data meets big brother. Orient BlackSwan Hyderabad, 2019.
Kodali, Srinivas. "From Birth to Death, Taking a Look at India's Real-Time Governance Dreams." *The Wire*, 23 December 2021, https://thewire.in/tech/birth-death-india-real-time-governance-dreams . Accessed 29 March 2022.

Kodali, Srinivas. "Hyderabad's 'Smart Policing' Project Is Simply Mass Surveillance in Disguise." *The Wire*, 8 February 2017, https://thewire.in/government/hyderabad-smart-policing-surveillance. Accessed 28 March 2022.

Kodali, Srinivas. "Why National Health ID without Laws Is Another 'Aadhaar Fiasco." https://www.thequint.com/voices/opinion/national-health-id-national-health-data-management-policy-aadhaar-data-privacy-information-technology-industry, *The Quint*, 10 September 2020, www.thequint.com/voices/opinion/national-health-id-national-health-data-management-policy-aadhaar-data-privacy-information-technology-industry.

Kovacs, Anja and Nayantara, Ranganathan. "Criminal law and freedom of expression on the internet in India", *Unshackling expression: A study on laws criminalising expression online in Asia*. Global Information Society Watch 2017 Special edition. APC. 50-82. https://giswatch.org/sites/default/files/giswspecial2017_web.pdf

Living in Digital Darkness: A Handbook on Internet Shutdowns in India. SFLC.in. May 2018. https://sflc.in/living-digital-darkness-handbook-internet-shutdowns-india

Mangona et al. "CENSORSHIP: THREATS TO DIGITAL EXPRESSION." *The Centre for Internet and Society, India Digital Freedoms Series*, October, 2020, https://cis-india.org/internet-governance/blog/india-digital-freedoms-3-censorship. Accessed 8 March 2022.

Marda, Vidushi, Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making. *Philosophical Transactions A: Mathematical, Physical and Engineering Sciences* (2018), https://ssrn.com/abstract=3240384.

Marquis-Boire, Morgan et al. "You Only Click Twice: Finfisher's Global Proliferation - Citizen Lab". *The Citizen Lab*, 13 March 2013, https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/. Accessed 5 March 2022.

"Media Policy-2020" *The Government Of Jammu And Kashmir, Information Department*, 15 May 2020. http://new.jkdirinf.in/images/MediaPolicy.pdf

"Ministry of I&B Order on Revocation of Uplink and Downlink Permission to Media One Channel Upheld by Kerala High Court". *Ministry of Information & Broadcasting, Press Information Bureau.* 8 February 2022. https://pib.gov.in/PressReleasePage.aspx?PRID=1796472

Nadaf, A.H. (2020). Digital Dissent and Censorship in the Kashmir Conflict. In: Jones, J., Trice, M. (eds) Platforms, Protests, and the Challenge of Networked Democracy. Rhetoric, Politics and Society. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-36525-7_16

Krishnan, Anjana. “India”, *Reuters Institute Digital News Report 2021*, 10th Edition, Reuters Institute for the Study of Journalism. 134-135. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf

Pahwa, Nikhil. “India’s Information Technology (Amendment) Bill Passed By Lok Sabha | Medianama”. *Medianama*, 23 December 2008, https://www.medianama.com/2008/12/223-indias-information-technology-amendment-bill-passed-by-lok-sabha/. Accessed 4 March 2022.

Parashar, Utpal. “Manipur Police orders monitoring of social media posts.” *Hindustan Times*, 22 July 2021, https://www.hindustantimes.com/india-news/manipur-police-orders-monitoring-of-social-media-posts-101626937184514.html. Accessed 3 March 2022.

Paul, VK, and Rajesh Bhushan. “National Family Health Survey (NFHS-5).” *District Level Household Survey*, 2021, http://rchiips.org/nfhs/factsheet_NFHS-5.shtml. Accessed 25 March 2022.

“Pegasus: Panel to Probe Spying Charges Submits Its Report to SC.” *The Indian Express*, 22 February 2022, indianexpress.com/article/india/pegasus-panel-to-probe-spying-charges-submits-its-report-to-sc-7784559/. Accessed 23 February 2022.

Planning Commission, Government of India. Government Of India, 2009, https://uidai.gov.in/images/notification_28_jan_2009.pdf. Accessed 8 Mar 2022.

Purnell, Newley and Jeff Horwitz. *The Wall Street Journal*, 14 August 2020, https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346 Accessed 17 Apr 2022.

Radhakrishnan, Radhika. *“I Took Allah’s Name and Stepped Out”: Bodies, Data And Embodied Experiences Of Surveillance And Control During COVID-19 In India*. The Internet Democracy Project, New Delhi, 2022, https://internetdemocracy.in/reports/i-took-allahs-name-and-stepped-out-bodies-data-and-embodied-experiences-of-surveillance-and-control-during-covid-19-in-india. Accessed 29 Feb 2022.

Ramanathan, Usha. “Biometrics Use For Social Protection Programmes In India Risk Violating Human Rights Of The Poor”. *Social Protection and Human Rights*, 2 May 2014, https://socialprotection-humanrights.org/expertcom/biometrics-use-for-social-protection-programmes-in-india-risk-violating-human-rights-of-the-poor/

Rao, Anuradha. “How Did Social Media Impact India’s 2019 General Election?”. *Economic And Political Weekly*, 2019, https://www.epw.in/engage/article/how-did-social-media-impact-india-2019-general-election.

Repucci, Sarah. “Media Freedom: A Downward Spiral.” *Freedom House*, 2019, https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downward-spiral. Accessed 25 March 2022.

Roth, Kenneth. *World Report 2022: India*. Human Rights Watch, 2022, https://www.hrw.org/world-report/2022/country-chapters/india.

“RSF Unveils 20/2020 List Of Press Freedom’S Digital Predators”. *Reporter’s without borders*, 12 March 2020. https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators.

Scott-Railton, John, et al. *Dark Basin Uncovering a Massive Hack-For-Hire Operation.* Citizen Lab Research Report No. 128, University of Toronto, June 2020. https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf

“SFLC.In Raises Concerns with reticent stakeholder consultation by the National Health Authority”. *SFLC.In*, 19 May 2021, https://sflc.in/sflcin-raises-concerns-reticent-stakeholder-consultation-national-health-authority.

Shekar, Kamesh, and Shefali Mehta. "The state of surveillance in India: National security at the cost of privacy?" *ORF*, 17 February 2022, https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/. Accessed 28 March 2022.

"State of Cyber Security and Surveillance in India a Review of the Legal Landscape." *The Centre For Internet and Society*, 9 February. 2022, cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf.

"Statements Issued." *Editors Guild of India*, https://editorsguild.in/statements-issued/. Accessed 25 March 2022.

"State of Privacy India". *Privacy International and the Centre for Internet and Society*, 26 January 2019, https://privacyinternational.org/state-privacy/1002/state-privacy-india#commssurveillance
Sinha, Amber. *Social Media Monitoring*. The Centre for Internet and Society, 2017, https://cis-india.org/internet-governance/blog/social-media-monitoring. Accessed 13 March 2022.

Singh, Kushagra et al. "How India Censors The Web". *12th ACM Conference On Web Science*, 2020. ACM, doi:10.1145/3394231.3397891. Accessed 7 Mar 2022.

Telecom Regulatory Authority of India. *DIGITAL COMMUNICATIONS The force multiplier in India's progress*, 31 May 2021, https://trai.gov.in/sites/default/files/ADC_31052021_1.pdf .

Telecom Regulatory Authority of India. *The Indian Telecom Services Performance Indicators*, July – September, 2021. 10 January 2022, https://www.trai.gov.in/sites/default/files/QPIR_10012022_0.pdf.

"The Aadhaar Judgment and the Constitution – I: Doctrinal Inconsistencies and a Constitutionalism of Convenience". *Indian Constitutional Law and Philosophy*, 28 September 2018, https://indconlawphil.wordpress.com/2018/09/28/the-aadhaar-judgment-and-the-constitution-i-doctrinal-inconsistencies-and-a-constitutionalism-of-convenience/. Accessed 1 Mar 2022.

"THE CONSTITUTION OF INDIA." *Legislative Department*, 9 September 2020, https://legislative.gov.in/sites/default/files/COI.pdf. Accessed 25 March 2022.

"The Wire: Heartland Hatewatch". *The Wire*, https://tools.thewire.in/hatewatch/speech. Accessed 10 March 2022.

Tiwari, Udbhav. "The Design & Technology behind India's Surveillance Programmes — The Centre for Internet and Society." *The Centre for Internet and Society*, 20 January 2017, https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes. Accessed 7 March 2022.

"Twitter, FB and others remove nearly 100 posts after govt order" *Times of India*. 25 April 2021.https://timesofindia.indiatimes.com/india/twitter-fb-and-others-remove-nearly-100-posts-after-govt-order/articleshow/82242666.cms. Accessed on 19 February.

Twitter. "Updates on our response to blocking orders from the Indian Government." *Twitter Blog*, 10 February 2021, https://blog.twitter.com/en_in/topics/company/2020/twitters-response-indian-government. Accessed 29 March 2022.

"UN Rights Experts urge India to end communications shutdown in Kashmir.", United Nations Human Rights Office of the High Commissioner. 22 August 2019, www.ohchr.org/en/press-releases/2019/08/un-rights-experts-urge-india-end-communications-shutdown-kashmir?LangID=E&NewsID=24909.

Vardarajan, Siddharth. "Revealed: How The Wire and Its Partners Cracked the Pegasus Project and What It Means for India." *The Wire*, 29 July 2021, https://thewire.in/media/revealed-how-the-wire-partners-cracked-pegasus-project-implications-india. Accessed 7 February 2022.

Venugopal, Vasudha. "What Led I&B Ministry To Decide On Withdrawing The Social Media Hub Proposal". *The Economic Times*, 3 August 2018, https://economictimes.indiatimes.com/news/politics-and-nation/what-led-ib-ministry-to-decide-on-withdrawing-the-social-media-hub-proposal/articleshow/65264159.cms?from=mdr. Accessed 13 Mar 2022.

Vijayakumar, Chithira, and Tanisha Ranjit. *Virus Detected: A Profile Of India's Emergent Ecosystem Of Networked Technologies To Tackle Covid-19*. Internet Democracy Project, New Delhi, 2021, https://internetdemocracy.in/reports/virus-detected. Accessed 22 Feb 2022.

Vivek Bhatnagar, Gaurav. "Aarogya Setu Data Was Made Available To J&K Police In Kulgam, Reveals RTI". *The Wire*, 2021, https://thewire.in/government/aarogya-setu-data-was-made-available-to-jk-police-in-kulgam-reveals-rti.

"Who Owns The Media In India ? | Media Ownership Monitor". *Media Ownership Monitor*, 2022, https://india.mom-rsf.org/.

"Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State." *The Wire*, 14 January 2019, thewire.in/law/supreme-court-pil-centre-snooping.

Woodhams, Samuel, and Simon Migliano. "The Global Cost of Internet Shutdowns 2021 Report." *Www.top10vpn.com*, 4 January 2022, www.top10vpn.com/research/cost-of-internet-shutdowns/2021/.

Xynou, Maria. "Big Democracy, Big Surveillance: India's Surveillance State." *OpenDemocracy*, 10 February 2014, www.opendemocracy.net/en/opensecurity/big-democracy-big-surveillance-indias-surveillance-state/.

GlobalVoices advox

The
Un~~freedom~~
Monitor