Check for updates

Article

new media & society
1–20
© The Author(s) 2023
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14614448231176552
journals.sagepub.com/home/nms
Sage

Contingent connectivity: Internet shutdowns and the infrastructural precarity of digital citizenship

Rohan Grover
University of Southern California, USA

Abstract

The Indian state has invested simultaneously in connectivity by pursuing universal Internet access and in disconnectivity by leading the world in state-ordered Internet shutdowns. How can we make sense of these contradictory approaches to technology policy? This article argues that this paradox illustrates a bifurcated experience of digital citizenship moderated infrastructurally through differential access to mobile connectivity. While previous research has largely interpreted Internet shutdowns as curtailments of freedom of expression, this article evaluates the implications for citizenship itself by bringing together scholarship on digital governance, science and technology studies (STS) approaches to Internet governance, and postcolonial and decolonial theory. More broadly, this article raises the stakes for critical analysis of how authoritarian states approach Internet policy to bridge digital divides—and for evaluating quality and contingency of connectivity experienced by marginalized and peripheral communities.

Keywords

Citizenship, digital divide, e-governance, infrastructure, Internet governance, Internet shutdowns

Introduction: a paradox of connectivity and disconnectivity

Two events in April 2020 collectively reveal a disjuncture in the Indian state's pursuit of universal Internet access. First, in response to the COVID-19 pandemic, the central

Corresponding author:
Rohan Grover, Annenberg School for Communication and Journalism, University of Southern California, 3502 Watt Way, Suite G4, Los Angeles, CA 90089, USA.
Email: rohan.grover@usc.edu

government launched a contact tracing mobile app called Aarogya Setu to spread public health information and alert users about their exposure to the virus. Its use was soon mandated for particular groups, including government workers, travelers, and delivery workers. Second, Kashmir was still emerging from the longest telecommunications blackout ever imposed by a government on its own people: starting in August 2019, people in Kashmir lived for nearly 6 months without phones, broadband, or mobile Internet after the central government unilaterally revoked the region's semi-autonomous status granted by Article 370 of the constitution. By April, only 2G access had been restored, leaving many people disconnected, including medical workers looking for updates about the emerging pandemic.

Each event is unsurprising, to a degree, on its own: Aarogya Setu is just one of a series of digital governance technologies launched under Prime Minister Narendra Modi's Digital India campaign, and Internet shutdowns have grown increasingly routine in India, which accounts for the majority of Internet shutdowns imposed worldwide each year since its first documented shutdown in 2011 (Access Now, 2019). Nevertheless, the conjunction of these two events highlights a tension between the Indian state's investments in *connectivity*—bridging the digital divide—and in *disconnectivity*, especially as they relate to the promises of citizenship in the digital age.[1] In particular, it is startling to see this clampdown of control alongside investments in expanding connectivity under the goal of bridging the digital divide.

How can we make sense of these two contradictory approaches to technology policy, expanding connectivity through Digital India on one hand while restricting connectivity by imposing Internet shutdowns on the other? This article argues that this paradox illustrates a bifurcated experience of citizenship moderated infrastructurally by differential access to mobile connectivity. This analysis addresses a gap in the literature in exploring the political stakes of Internet shutdowns. While previous research has largely interpreted Internet shutdowns as curtailments of freedom of expression, this article evaluates the implications for citizenship itself by bringing together scholarship on digital governance, science and technology studies (STS) approaches to Internet governance, and postcolonial and decolonial theory. More broadly, this article raises the stakes for critical analysis of how authoritarian states approach Internet policy to bridge the digital divide—and for evaluating the quality and contingency of connectivity experienced by for marginalized and peripheral communities.

The article proceeds as follows. It begins by situating the analysis in the contemporary political context of "Digital India," Narendra Modi's campaign to advance a technopolitical vision for the state, and its implications for an evolving citizenship regime and mobile Internet specifically as a mode of governance. It then reviews recent analyses of Internet shutdowns and identifies a gap in reconciling the unparalleled frequency and intensity of shutdowns with investments in connectivity. Next, it draws on STS approaches to Internet governance to construct a theoretical framework to unpack the "black box" of Internet shutdowns by "following the infrastructure" when a shutdown is imposed and evaluating disparate impacts on marginalized and peripheral communities. The article thus applies actor-network theory to legal and political economic analyses to identify infrastructural control points in the process of enacting a shutdown, and evaluates a ledger of shutdowns from the Software Freedom Law Center (SFLC) to identify

disparate impacts. Finally, it identifies "m-governance" as a political technopolitical regime to make sense of the paradox of dis/connectivity, and discuss its implications, including bifurcating the public and sowing acquiescence through the mundanity of Internet shutdowns.

Citizenship in Digital India

This article approaches Internet shutdowns within the context of the Indian government's embrace of e-governance and the resulting implications for citizenship in the country. Narendra Modi launched the Digital India campaign in 2015 to "transform India into a digitally empowered society and knowledge economy" (Digital India, n.d.) through sustained investment in digital governance. The vision was articulated through three strategies: increasing Internet connectivity as digital infrastructure for all citizens, investing in e-governance by digitizing government operations and services, and increasing digital literacy to support citizens in helping themselves avail government services and pursue economic opportunities.

The Aadhaar program illustrates the stakes and scale of transformation under Digital India. Aadhaar is a program intended to provide a single national unified mechanism for identification and verification throughout India based on biometric and biographical data. Although its conceptualization predated Modi's term as prime minister, its launch was marketed as a Digital India initiative through advancing digital governance, followed a decades-long vision for a unique, universal identification scheme to enable accurate identity and address authentication by storing biodata in a centralized database that can not only be linked to government services but also facilitate economic transactions and national security surveillance (Rao and Nair, 2019).

Chaudhuri and König (2018) have operationalized the conceptual framework of a *citizenship regime* to evaluate Aadhaar as a technology of governmentality that fundamentally shapes both the criteria and experiences of citizenship. Their analysis is based on Jenson's (2007) concept of a citizenship regime, which draws on Foucault's concept of governmentality to define a paradigm consisting of "institutional arrangements, rules and understandings that guide and shape concurrent policy decisions and expenditures of states, problem definitions by states and citizens, and claims-making by citizens" (p. 55) that collectively define citizenship in a particular national context. There are four dimensions to a citizenship regime: responsibility mix, rights and duties, governance arrangements, and the definition of membership. They have argued that Aadhaar reimagined the Indian citizenship regime by redefining the boundaries of inclusion and exclusion and especially by displacing analog modes of eligibility and claims-making with digital alternatives. Thus, Aadhaar has emerged as not only a technological intervention but also as a site of contested citizenship, with eligibility for access to governmentality moving from an inclusive model to an exclusive one, transforming citizens into subjects. Under this framework, Aadhaar signals the transformation of at least two dimensions of India's citizenship regime. In terms of responsibility mix, the state now acts more as a platform that provides infrastructure to facilitate provision of welfare and other services by non-state private actors (Chaudhuri and König, 2018; Rao and Nair, 2019). In terms of governance arrangements, or the "institutional mechanisms and modes of participation through

which access to the state is made possible, and specific types of claim-making are legitimized" (Chaudhuri and König, 2018: 138), Aadhaar represents a comprehensive turn to digital mediation of citizen participation. This includes formal engagement with the state through accessing welfare and other services as well as private forms of citizenship, as Aadhaar comprises the basis for the "India Stack," a series of application programming interface (API)-based applications intended to assist companies with digital identity authentication, cashless payments, and other transactions (Dattani, 2021). These forms of "techno-authentication" are a burden for marginalized populations to engage in full civic participation (Gurumurthy et al., 2017: 48–49).

The technological mediation of citizenship is understood as a form of *digital citizenship*. In India, this mode of digital citizenship is made explicit by programs such as Aadhaar under the Digital India regime, but it is not specific to India alone. This approach contrasts with conceptualizations of digital citizenship as participation in society in a general sense (e.g. Mossberger et al., 2007). Instead, the citizenship regime framework illuminates how the state's implementation of Digital India carries significant implications for citizen–state relations by reconfiguring who is able to access rights and benefits from the state. In other words, in a digital citizenship regime such as Digital India, digital connectivity is not only ideal but in fact necessary to fully participate in political, economic, and civic life.

Mobile Internet: a "passport to Republic of Digital India"

Through Digital India, Modi has articulated a mobile-first digital governance strategy that he has referred to as *m-governance*, or "mobile governance," which directs technological governmentality to the modality of mobile phones. For example, 6 months before launching Digital India, Modi highlighted mobile devices as a crucial mode of expanding connectivity. He tweeted: "I urge you to explore ways to provide as many services as possible through mobiles. Let us bring the world into our mobile phones!" followed by, "While we look at e-governance, let us think about 'mobile first' and thus give importance to m-governance" (IANS, 2015).

While m-governance lacks a formal definition, this article interprets it as a technopolitical policy framework that prioritizes mobile modes of delivering information, affording rights, and administering welfare and other services. For example, in his articulation of connectivity as the first of three strategies under Digital India, Modi included the initiative to extend broadband service to rural communities begun by his Congress party predecessors in 2011, but pointed specifically to mobile Internet as the focus for universal connectivity. In addition, in the launch event he again stressed the importance of mobile Internet not only for connectivity but as a mode of governance: "We have to move from e-governance to m-governance" (Press Trust of India (PTI), 2015: 5).

The rapid deployment of Aarogya Setu serves as another example of m-governance in action. The app was launched by the Ministry of Electronics and Information Technology (MeitY) in April 2020 to implement a digitized COVID-19 mitigation strategy. It communicated with a central database recording positive COVID-19 cases, sending self-reported positive cases and reading data from the Indian Council of Medical Research database to alert users based on their location history (Basu, 2021). Despite concerns

about poor privacy and security safeguards articulated by digital rights organizations and reported by journalists, the app was imposed as an essentialized technology of not only utility and public health but also as a condition for realizing the full experience of citizenship, including mobility and employment. These technopolitical applications of Aarogya Setu demonstrate how mobile governance can be enacted to reconfigure governance arrangements in India's citizen regime.

M-governance also carries implications for India's telecommunications industry, which has been characterized as porous to business interests. This has been discussed at length in the broader context of crony capitalism in India (e.g. Sinha, 2019), and specifically in telecom (e.g. Bhatia, 2019; Thakurta and Kaushal, 2010). In particular, multinational conglomerate Reliance Industries has been scrutinized for securing special access and political favors through relationships with political elites (e.g. Caussat, 2017; Thakurta et al., 2014). Further evidence can be found in the public narrative of m-governance. For example, when Reliance launched a telecommunications subsidiary, Jio, in 2016, founder Mukesh Ambani described it as "a dedication to that Digital India dream of the Prime Minister, his vision for the 1.2 billion people of India" (*Financial Express*, 2016). The launch featured an advertising campaign that described the JioPhone as the "passport to [the] Republic of Digital India" (Spike Asia, n.d.). Reliance Jio also purchased full-page ads on the front page of national daily newspapers such as the *Times of India* and the *Hindustan Times*, displaying Modi's image and the Jio logo connected by the phrase "Dedicated to India and 1.2 billion Indians" (Baxter, 2016). Despite widespread criticism for using the Prime Minister's name and likeness in an advertisement (*Deccan Chronicle*, 2016), Modi did not admonish Jio for these ads, conveying tacit approving of Jio and its contribution to Digital India (Baxter, 2016). Jio later acknowledged to the consumer affairs ministry as an "inadvertent mistake," claiming that the intent was to celebrate Modi's initiative rather than market their product (*Hindustan Times*, 2017). Ultimately, the campaign can be seen as an unusually public acknowledgment of the informal alliance between business and political elites that has bolstered Digital India.

Jio's entrance to the telecommunications market also marked an inflection point in the growth of mobile Internet access in India. Unlike its competitors, Jio leveraged Reliance's assets to strategically pursue long-term universal Internet access at the expense of short-term profits, only months after Facebook failed to achieve the same goal with Free Basics.[2] Jio introduced the country's first 4G network, undercut competitors' rates, and offered the first unlimited data plan (Singh, 2020a). This combination of factors both attracted customers from competitors and expanded the market of mobile Internet users: Jio gained 400 million subscribers over 5 years to become the largest mobile network in the country, and the second largest in the world, in 2020 (Singh, 2020a). This was achieved by marketing Jio as uniquely accessible to the average Indian, so the company offered free voice calls and data, with generous mobile data limits, to every customer who subscribed shortly after it launched in 2016. Consequently, Jio's competitors also dropped their prices to retain customers, collectively driving a 95% reduction in mobile Internet costs from 2013 to 2019, which resulted in the cheapest mobile data prices in the world (Roy, 2019). Prior to 2016, most mobile Internet users in India relied on 2G technology (Shu, 2015), and only 9% of rural Indians had access to the Internet (Internet and

Mobile Association of India (IAMAI), 2015), whereas in 2019, 85% of rural and urban Indians had access to 4G Internet (IAMAI, 2019). More recently, in 2020 Jio received significant foreign investment, bolstering its financial standing in the Indian telecom space: both Google and Facebook announced separate US$4.5 and US$5.7 billion investments within months of each other (Singh, 2020a, 2020b)—the latest of a series of investment attempts over several years to capture the growing Internet connectivity market in India, especially after the spectacular failure of Facebook's Free Basics succumbed to pressure from civil society advocacy driven by information technology (IT) workers (Prasad, 2018).

The world leader in Internet shutdowns

The centrality of Internet connectivity to civic life in Digital India underscores the instability incurred by imposed disconnectivity in the form of Internet shutdowns. Against the articulation of Digital India bringing about a digitally empowered society through expanded connectivity and governmental and economic digitization, Indians have nonetheless endured the most intense frequency and severity of Internet shutdowns in the world. They have grown increasingly common since the first documented shutdown in 2011; recently, India has accounted for the majority of Internet shutdowns imposed worldwide each year (Access Now, 2022). In economic terms, the Indian Council for Research on International Economic Relations estimates the impact of 16,315 hours of Internet shutdowns between 2012 and 2017 to be US$3.04 billion (Kathuria et al., 2018).

The recent spike in Internet shutdowns has inspired a surge in research that is beginning to unpack how and when they are imposed and to understand people's experiences on the ground. While the earliest scholarship has framed Internet shutdowns as censorship to curtail freedom of expression (Deibert et al., 2008; Howard et al., 2011), more recently scholars have argued that Internet shutdowns should be understood as more fundamental issues of human rights because of their impact on a variety of rights including freedom of information and freedom of assembly. In particular, Wagner (2018) has examined Internet shutdowns in Pakistan and found that they often correlate with political events such as rallies and elections. He therefore argues that Internet shutdowns are intended to create "communication ruptures" that sabotage the public's ability to hold the state accountable for its actions, and they often target marginalized communities to "discipline" them against mobilizing against the state. In India, meanwhile, government officials often identify "communal tension," "national security," and other "public order reasons" as the rationales to impose Internet shutdowns (Nazmi, 2019; Pankaj, 2022). While most shutdown orders cannot be attributed to specific central or state government actors, the volatile political climate overall can be traced back to efforts to stoke communal tension by the Bharatiya Janata Party (BJP) and its affiliated network of Hindu nationalist organizations known as the *Sangh Parivar* (Ruijgrok, 2022).

Studying Internet shutdowns is complicated by the fact that the true number of events is unknowable. Shutdown orders may be classified as "top secret," and therefore would be exempt from public disclosure (Nayak, 2018), and government officials have admitted to not maintaining accurate ledgers (Nayak, 2018; SFLC, 2018). (This obscurity further betrays Digital India's promise for greater transparency.) In the absence of an

official record, the public relies on the press to document when Internet shutdowns occur, what telecommunications services or platforms are affected, their geographic scope, and any motivations claimed by public officials or telecom operators who may disclose the orders to journalists. SFLC collects such news articles in a public log named the Internet Shutdown Tracker[3] which serves as the most comprehensive archive of Internet shutdowns in India.

Therefore, the extent of Internet shutdowns that go unrecorded is unknown, but two examples may indicate the true scale. In 2018, SFLC recorded 14 Internet shutdowns in the state of Rajasthan between July 2017 and January 2018 based on reports documented by the news media. The state government ultimately acknowledged that in fact 40 incidents—nearly three times as many—had occurred, although details about the vast majority of them were still classified (SFLC, 2018). In addition, in a series of interviews, women in Manipur reported experiencing four Internet shutdowns between 2015 and 2017, but only two of the four had ever been documented in the English-language press and could not be independently verified years later (SK and Lakshané, 2018). According to these two assessments, the actual number of shutdowns enacted may be two to three times the number recorded by SFLC.

It is important to note that Internet shutdowns are not enacted centrally or uniformly. There has never been a shutdown across the entire nation; instead, they are imposed within state or local jurisdictions (Ruijgrok, 2022). Furthermore, Parray (2021) reminds us to resist the urge to resort to an oversimplified national narrative in which Internet shutdowns affect populations equally, and instead to distinguish between the broad categories of the heartland, where the Internet is abundant with opportunity, and the periphery, where it is a tool for oppression.

There is no indication that Internet shutdowns will decrease in frequency or severity in the near future, and so the paradox of governmental embrace of connectivity while simultaneously imposing regular disconnectivity calls for deeper analysis to reconcile these two approaches. Moreover, the implementation of Internet shutdowns mobilizes a network of sociotechnical and regulatory actors with different visibilities and histories. Therefore, this article draws from a science and technology studies (STS) toolbox, especially as applied to Internet governance scholarship, to assess the political dynamics and implications of Internet shutdowns.

Unpacking Internet shutdowns

This article contributes to the growing body of scholarship on Internet shutdowns by bringing the analytic disposition and tools of STS, following Internet governance scholars (e.g. Epstein et al., 2016; Musiani, 2015), guided by a commitment to decolonial computing. Ali (2016) defines decolonial computing as a critical project of centering political economy to "interrogat[e] who is doing computing, where they are doing it, and, thereby, what computing means" that is "informed by (even if not situated at) the margins or periphery of the modern world system wherein issues of body politics and geopolitics are analytically foregrounded" (p. 20). In practice, this means prioritizing specificity in tracing the actors and interests implicated in enacting a shutdown and

evaluating who is most impacted by Internet shutdowns rather than assessing national costs or calculating impact on the average Indian.

This article follows an infrastructure-based approach to Internet governance that looks beyond content to understand how technical architecture and other infrastructures mediate and encode value frameworks, actor positionalities, and hierarchies of power within a sociotechnical system (DeNardis, 2012; Musiani et al., 2016). Specifically, following DeNardis (2012), it searches for "control points" in the network where values are mediated and contested. This approach builds on recent Internet governance scholarship that avoids overly particularistic focus on the state alone or individuals as the level of analysis (Epstein et al., 2016). Instead, it "follows the infrastructure" (Cowen, 2020) to explore how India's system of dis/connectivity brings nonhuman infrastructural actors to the fore (Musiani et al., 2016). Empirically, it draws from legal analyses of Internet shutdowns and mapping political economic relations between the telecom industry and the Indian state to illustrate how connectivity and disconnectivity is mediated as it passes through the network. By focusing on legal and technical infrastructures, this article is able to discern the values that are being preserved and inscribed. Analytically, it draws on Akrich's (1992) vocabulary of various *scripts* to understand how different actors—in this case, the state(s), Internet service providers (ISPs), citizens, and legal mechanisms—interact with and upon each other. In other words, which components of the network compel different actors to act and to be acted upon by either encoding durable political subjectivities (in-scription), imposing expectations upon other actors (pre-scription), or complying with those expectations (sub-scription)?

This analytic process begins with defining, mapping, and evaluating—or de-scribing (Akrich, 1992)—the network itself.[4] To do this, this article first evaluates a ledger of Internet shutdowns maintained by SFLC (2020) to assess the uneven impact of Internet shutdowns among different communities. SFLC supplements news reports with Right to Information (RTI)[5] requests and reports by individuals that are verified before being added to the tracker (SFLC, 2018). The archive includes metadata such as which telecommunications services or platforms are affected by a shutdown, its geographic scope, and any motivations claimed by public officials or telecom operators who may disclose the orders to journalists. Finally, this article builds on Chaudhuri and König's (2018) application of the "citizenship regime" framework, as described previously, to evaluate how Internet shutdowns represent a shift to citizen–state relations—especially amid the broader context of technological mediation that produces an experience of digital citizenship. In particular, it is concerned with how Internet shutdowns reveal technopolitical changes to governance arrangements—the second dimension in the framework—which refers to shifts in an individual's ability to access, participate in, and benefit from the state.

De-scribing Internet shutdowns

Following the infrastructure

This section "follows the infrastructure" through two key categories of actants implicated by the state's issuing of an Internet shutdown: the statutory apparatus and

telecommunications companies. It draws on legal analysis to map how various legal and regulatory statutes enable Internet shutdowns by sanctioning particular configurations of state power inscribed within them. In general, the central and state governments have derived their legal basis to issue Internet shutdown orders from three statutes: Section 144 of the Code of Criminal Procedure of 1973 ("Section 144"); Section 69A of the Information Technology Act of 2008 ("Section 69A"); and Section 5(2) of the Telegraph Act of 1885 ("Telegraph Act") (Bhardwaj et al., 2020). The priority among these three statutes has changed over time with both the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 ("Suspension Rules") and the Supreme Court case of *Anuradha Bhasin vs Union of India* marking crucial inflection points.

Before 2017, statutory authority to impose a shutdown was ambiguous, but most state actors—whether the central or state government—drew on Section 144 which empowers district and other executive magistrates to "direct any person to abstain from a certain act" in response to an urgent emergency circumstance with grave consequences (Bhardwaj et al., 2020). Section 144 imposes less cumbersome procedural requirements since it is most often used to mitigate public dangers or nuisance and thus only requires an officer to testify to this fact (Bhardwaj et al., 2020). In comparison, Section 69A permits blocking access to specific sites, but it is a more limited statutory basis because it does not permit wholesale Internet shutdowns and it is only available to the central government.

In 2017, the central Department of Telecommunications (DoT) published the first dedicated rules to regulate Internet shutdowns. The Suspension Rules drew on the authority granted by the Telegraph Act. It represented a legitimation of Internet shutdowns by explicitly enumerating rules for suspending Internet access which included, for the first time, procedural safeguards (Nayak, 2018). For example, the Suspension Rules clarified that shutdown orders could only be issued by the Union or State Home Secretary and must be promptly submitted to, and within 5 days approved by, a review committee that assesses whether the orders are an appropriate response to a public emergency or threat to public safety (Bhardwaj et al., 2020).

The Telegraph Act is noteworthy for not only providing the legal basis for issuing shutdown orders, but also for its colonial legacy as an instrument of political control. Nayak (2018) notes that the Telegraph Act permits disrupting telegraph messages in the "occurrence of any public emergency or in the interest of the public safety" (8), which he characterizes as "lofty standards of public distress" (9) that allows for outlandish claims by the central government—such as preventing cheating on school exams—to justify an Internet shutdown in the name of "control." Moreover, this interpretation of the "public emergency or . . . public safety," despite its overly broad interpretation by the state, cannot be contested by the public because it is enshrined in law.

Both the Telegraph Act and Section 144 should be acknowledged as colonial legacies that perpetuate centralized power arrangements. Both statutes have been sustained from the imperial code imposed by the British during India's colonial era. In addition, the Indian government's use of each statute to impose Internet shutdowns represents a dramatic escalation in a colonial style of governance that transforms citizens into subjects. Section 144 was drafted to empower the state to respond to threats to public safety, which ostensibly occurred in traditional public spaces such as parks in the colonial era.

Meanwhile, the Telegraph Act regulated telegraphic transmissions—specifically an individual "message" (Bhardwaj et al., 2020: 17). Yet Bhardwaj et al. (2020) note that the term "message" was defined broadly as "any communication sent by telegraph or given to a telegraph officer to be sent by telegraph or to be delivered" (Telegraph Act of 1885). Thus, to the extent that accessing the Internet is tantamount to sending and receiving individual packets of data that contain a communicative value, in an Internet shutdown the Telegraph Act is actually being imposed upon each individual packet of data rather than on a general status of Internet connectivity. These draconian applications of colonial statutes therefore represent not only a continuity but in fact an escalation of a colonial mode of technopolitical subjectivity.

In 2020, the Supreme Court of India further refined the statutory authority for issuing Internet shutdown orders in the case of *Anuradha Bhasin vs. Union of India*. Bhasin, executive editor of the *Kashmir Times*, had filed the case because the longstanding Internet shutdown following the abrogation of Section 370 (described earlier in this article) interfered with the press. The court ruled that an indefinite suspension of Internet services is unlawful because the Internet is a medium through which individuals exercise the right to freedom of expression; and since this right is guaranteed by Article 19 of the Constitution, an indefinite shutdown violates a constitutional right. Thus, the ruling imposed several procedural safeguards on the Suspension Rules: that shutdown orders must be published, temporary, proportionate, and subject to review. It also affirmed that shutdown orders must be issued using the Suspension Rules rather than Section 144. However, according to digital rights advocates, there have been many examples of Internet shutdowns since 2020 that have violated the *Anurabha Bhasin* ruling (see Internet Freedom Foundation [IFF], 2021).

Once the state has drawn upon one of the three statutes to impose an Internet shutdown, responsibility is then transferred to telecom providers to enact the order. Nayak (2018) notes that it is surprising that telecom companies do not resist these orders, especially given their extreme economic costs cited earlier. However, the regulatory context reveals why telecom providers are compelled to oblige, and the political economy of telecom service illuminates why profits may not be the most compelling factor.

In 1994, the telecom industry was liberalized through the National Telecom Policy, which laid the groundwork for private enterprises to offer private wired and wireless telecommunications services (Subramanian, 2020). Subramanian describes how these private operators were not exempt from government surveillance because they were authorized to provide connectivity services through licenses that imposed specific requirements, including an obligation to supply intelligence agencies with activity logs upon request. Nayak (2018) adds that the licenses further stipulate that operators must terminate service in designated areas within 6 hours of a government request—such as a shutdown order. Licenses are granted only by the central government, so such suspension orders come from the Department of Telecommunications (Chari, 2014).

These stipulations are enforced both in terms of the license, which permits penalties up to Rs. 50 crore (between US$6.5 and US$7 million) per service area, and in the Telegraph Act, which permits the government to suspend or revoke a license (Nayak, 2018). For example, when a 3-day mobile Internet shutdown was imposed in the city of Vadodara, Gujarat, in 2014, compliance was further enforced by the police invoking

Section 188 of the Indian Penal Code, which is used to ensure obedience to an order by a public servant (Chari, 2014). Nayak (2018) notes that telecom operators are also legally accountable to the public because spectrum is considered a natural resource administered by the government on behalf of the people. Nevertheless, public accountability has not been exercised in opposition to Internet shutdowns.

While nearly all Internet subscribers in India use private ISPs, it is important to also consider how Internet shutdowns may differentially affect state-owned Internet service. As of 2019, three private companies—Reliance Jio, Bharti Airtel, and Vodafone Idea—served 95% of Indians (TRAI, 2020). This leaves less than 5% of subscribers gaining Internet access through state-owned telecom services, namely Bharat Sanchar Nigam Limited (BSNL) and Mahanagar Telephone Nigam Limited (MTNL), and there is some evidence that they are treated differently from private telcos. For example, one study by the Bachchao Project found that BSNL subscribers were able to access low-quality Internet while private services were fully disabled during a state-ordered shutdown (SK and Lakshané, 2018). The authors propose several potential explanations, including: BSNL services were retained to power the backbone of government connectivity networks; private telcos over-complied with ambiguous government orders; or the government provided different orders to BSNL and private telcos for any number of reasons. The justification for differential enforcement across private and public telco services remains largely undocumented, but nonetheless merits further exploration.

The relationship between telecom companies and the state(s) therefore provides a crucial basis for Internet shutdowns to be enacted. The strength of this relationship can be evaluated in the context of the Modi government's investment in m-governance under the Digital India campaign. Thus, although telecom companies face significant revenue loss, the state wields its power through both economic and legal mechanisms (see Mare, 2020).

Disparate impacts on communities

This section focuses on the implications of disconnectivity imposed by Internet shutdowns: who is affected and how? It analyzes Internet shutdowns as moments of not only disconnectivity but also disenfranchisement of select communities, distinguishing between communities with stable, reliance connectivity to both Internet and citizenship, and communities susceptible to state control through Internet shutdowns. The purpose of this analysis is to understand what "work" is achieved by Internet shutdowns in order to evaluate the network described earlier.

This section analyzes SFLC's (2020) Internet shutdowns tracker as an historical ledger to show that Internet shutdowns are sites of heterogeneous disconnectivities that amount to disenfranchisement imposed unequally upon communities on the basis of mobile connectivity access, geography, and political speech. These data illuminate how m-governance can be understood as a technopolitical regime that features predatory inclusion to render new populations susceptible to Internet shutdowns as state-operated levers of political control.

The first dimension is the mode of connectivity. Every single shutdown in the ledger has affected mobile Internet services. Among the shutdowns recorded by SFLC, 85%

have affected mobile Internet alone, 14% have affected both mobile Internet and broadband, and 1% have affected broadband only but were imposed during existing mobile Internet shutdowns. The disproportionate focus on mobile Internet users represents the most dramatic discrepancy, and it retraces inequalities experienced by low-income and rural communities.

Internet shutdowns are also imposed more often in rural regions than in urban areas. Only 8% of shutdowns affected urban districts, 7% were statewide, and the vast majority (85%) affected rural districts only. *Gram panchayats*, or village councils, are the most local level for villages in a tiered democratic system. It is the oldest form of local governance in India, originally envisioned to serve as the backbone for a decentralized Indian national political system (Sharma and Singh, 2008). Instead, a highly centralized government was formed, with *gram panchayats* seen as local modulating forces to represent villages as political units. Therefore it is noteworthy that, while the Digital India vision initially articulated in 2015 included a "broadband highway" to provide *gram panchayats* with broadband Internet access via optical fiber cables, investment in rural connectivity has been instead focused on mobile Internet access through the private telecom industry (Kaka et al., 2019). Held against the disproportional imposition of Internet shutdowns on rural areas, this trend poses a challenge to local governance (SK and Lakshané, 2018).

Internet shutdowns have also been imposed unequally across the country, with Kashmir impacted most, followed by West Bengal and the North-East region. A recent inflection point was the longest comprehensive communications shutdown ever, imposed in August 2019 for nearly 6 months in Kashmir after revoking the state's semi-autonomous status. Indeed, the documented reasons why each shutdown was imposed, as reported in the press, also reveal a dimension of disenfranchisement by stifling political activity. For example, 61% of shutdowns were supposedly imposed preventatively—in anticipation of unrest or violence that had not yet occurred—with the rest imposed in response to existing events. Among shutdowns with motivations reported in the media, 35% were attributed to protests, political backlash, or terrorism. However, even when Internet shutdowns are acknowledged by public officials, the stated motivations cannot always be trusted. An analysis by the #KeepItOn coalition of advocacy organizations demonstrated that governments claim to shut down Internet access due to threats to public safety most often, followed by national security and fake news/hate speech; however Internet shutdowns were in reality initiated to stifle protest activity, communal violence, and political instability (Access Now, 2019). At the same time, the increase in Internet shutdowns in cosmopolitan regions, including, notably, Delhi's first shutdown in 2019, suggests that Kashmir is being used as a laboratory to experiment with repressive tactics that will inevitably be deployed across the country, albeit still unequally.

M-governance in an evolving citizenship regime

If "arrangements of technical architecture are also arrangements of power" (DeNardis, 2012), then what forms of power are embedded in the infrastructure mobilized to enact an Internet shutdown? This section identifies m-governance as a technopolitical regime (Hecht, 2009) to understand how particular infrastructural relations encode dynamics of power and control in Indian governmentality that undermines experiences of citizenship.

Clearly, m-governance is prominent in the state's investments in both connectivity and disconnectivity. On one hand, the state has invested specifically in mobile connectivity, especially since 2016 with the launch of Reliance Jio, which disrupted the mobile Internet market by rapidly expanding the market while setting record-low prices. On the other hand, mobile connectivity is the primary target of Internet shutdowns.

Therefore, this article conceptualizes m-governance as a technopolitical regime that now comprises another core feature of India's citizenship regime, which has four dimensions: governance arrangements, responsibility mix, rights and duties, and definition of membership (Chaudhuri and König, 2018; Jenson, 2007). Specifically, m-governance represents a governance arrangement in which the state modulates mobile connectivity to control access to citizenship, shaping individuals' access to both the state specifically and, broadly, to full civic life through various processes that require digital authentication, verification, or other modes of connectivity. These processes constitute a novel assemblage of rights and duties that form critical gatekeeping functions of citizenship, even though private ISPs bear the responsibility of provisioning access. The centrality of these processes carries implications not only for how citizens are "disciplined" through imposed digital mediation of citizen-state relations but also how membership in the citizenry is defined through digital access, literacy, and stability.

How do these transformations of the citizenship regime take place? The following section describes two key infrastructures of m-governance identified in the network analysis above: telecommunications companies and the statutory apparatus.

Key infrastructures of m-governance

Telecommunications companies. One striking implication of the network analysis is that telecommunications companies play a key role in operationalizing Internet shutdowns. This aligns with Vargas-Leon's (2016) assertion that a single "kill switch" does not actually exist; instead, Internet shutdowns are imposed through individual ISPs whose implementations may be distinct, either due to their own interpretation or simply different operational procedures. For example, Shah (2021) has characterized Internet shutdowns as "leaky" in that ISPs implement them at different times and do not always affect broadband and dial-up Internet connections, or where certain apps such as WhatsApp continue to function as normal. He has also described instances where individuals were unaware that their region was experiencing a shutdown until notified by friends or family.

Why do ISPs comply with shutdown orders? Freyburg and Garbe (2018) have argued that adherence can be explained by states' control over connectivity not only by owning physical telecommunications infrastructure but also by exercising regulatory control over ISPs. Thus, in the case of Zimbabwe, for example, telecommunications companies were likely to comply with Internet shutdown orders to retain their licenses and to avoid political harassment (Mare, 2020). The situation in India is likely similar. Furthermore, given the crony capitalism in India's telecommunications industry discussed earlier, the broader relationship between the state and telecom companies—beyond licensing alone—is key to understanding how Internet shutdown orders are passed between these actors.

Statutory apparatus. The previous section has shown how Section 144 has often been used to justify Internet shutdowns, supposedly in order to prevent unrest. Legal scholars have argued that the Indian state has chosen to draw from, interpret, and enforce this colonial-era statute as heavily as it does because:

> The provincial government led by Indians continued the colonial art of governance by resorting to repression as a significant tool to deal with political unrest . . . Some individuals or groups were marked as problem categories, that is individuals or a group who were identified by the colonial administration as a threat to peaceful governance and the maintenance of public order . . . Identifying a problem category was crucial to the colonial state to justify the creation as well as the invocation of repressive laws . . . The state tends to reduce the narrative of "public order" to a single model of unidimensional determination of power that in turn tends to either constrain or productively modify the political and moral meaning of various acts. (Wani, 2022: 23)

Wani's analysis shows that while Section 144 carries forward historical citizen-state relations from the colonial era, it is in fact animated by its particular use by the state to exercise control over certain populations and under certain circumstances. As Grover (2021) puts it:

> The constitutional transition of people from "subjects" to "citizens" led to the evolution and recognition of a new spectrum of rights, but did not see a parallel reorientation and sensitisation of the state machinery and its agents to the said rights. (p. 43)

Therefore, Section 144 is given its meaning by repeated patterns of use, demonstrating both the durability of colonial legal infrastructures and their interpretive flexibility in reacting to the "fear of the crowd" (Kumar, 2021).

Implications for citizenship

Bifurcating the public. Conditioning rights of digital citizenship on mobile Internet connectivity creates hierarchies based on contingencies imposed by the state itself. One hierarchy is based on political contestation: communities with oppositional politics to the state are targeted with Internet shutdowns, especially in Kashmir and the North-East. A second hierarchy is based on modes of connectivity: those with broadband Internet access are privileged to retain at least partial connectivity (in the form of broadband, for example) amid an Internet shutdown and therefore enjoy consistent access to government and citizenship services.

This digitally mediated bifurcation of the public evokes Mamdani's (1996) analysis of indirect rule in postcolonial states, in which the public was bifurcated into two populations: citizens and subjects. Citizens were members of the colonial state or elite, Western-educated, urban people from the colonized territories, and they enjoyed representation through organized civil society structures that afforded them a degree of political agency. Subjects, on the other hand, were the colonized natives who were relegated to indirect, often tribal administration. According to Mamdani, subjects "may have a modicum of civil rights, but not political rights, for a propertied franchise separated the civilized from

the uncivilized" (17). While Internet shutdowns do not amount to differential legal codes in the exact way Mamdani describes, they reveal a technologically mediated bifurcation in political agency that reifies historical differences on geographic, ethnic, caste, and class lines. The division is not exact: for example, rural areas are not the exclusive target of Internet shutdowns, and alleged reasons vary widely from punishing dissent or preemptively thwarting protest to curbing the spread of information. However, select inequalities stand out from the previous section: the intensity and frequency of shutdowns imposed on Kashmir and Darjeeling as laboratories for experimentation; the concentration of shutdowns in rural communities, and above all the universal imposition on mobile Internet.

Pre-scribing acquiescence through predatory connectivity. The state's simultaneous investment in connectivity and disconnectivity raises questions about the political utility of mobile Internet access. Against both the state's articulation of Digital India as promoting transparency and accessibility, and broader assumptions about the Internet's relationship to collective action, the imposition of Internet shutdowns suggests that Internet access can in fact render communities *more* susceptible to authoritarian intervention. This conceptualization suggests that mobile Internet can serve an instrumental value for regimes to exercise greater control over populations by serving as infrastructure of an authoritarian technopolitical regime, and therefore invites skepticism about digital divide initiatives as potential vehicles of predatory inclusion.

The stakes for predatory connectivity are raised by patterns of targeting Internet shutdowns to certain communities which could habituate them to contingent connectivity. In other words, the synthesized work of the network's actors and infrastructures—the state, telecom companies, and the statutory apparatus—effectively *pre-scribes* acquiescence to unstable access to citizenship to people in Kashmir, Darjeeling, the North-East, and other heavily targeted communities.

This pre-scription is analogous to the effect of load shedding, the routine practice of preemptively shutting electricity supply to sustain the stability of the system, on political resignation. Internet shutdowns represent similar exercises of preemptively cutting supply to sustain the stability of the broader technopolitical network. The Indian public is broadly conditioned to precarious electricity supply—although a hierarchy remains in the form of differential access to alternate energy sources, such as inverters or uninterruptible power supply units. Similarly, people with access to broadband, satellite, or other Internet sources are able to evade complete disconnection; for the rest, there is a risk that Internet shutdowns and disconnectivity will be considered increasingly mundane.

Unlike load shedding, of course, Internet shutdowns are imposed in a politically targeted way, representing a more nefarious bifurcation based not only on geography, but also on political subjectivity, to undermine experiences of citizenship in terms of citizen-state relations. In addition, Internet shutdowns are not caused by insufficient supply, but rather represent an excess of power. Against concerns that the global South is unprepared for digitalization due to insufficient regulations and infrastructure (Schia, 2018), this analysis of Internet shutdowns reveals that India is, in fact, quite well prepared to wield its technopolitical infrastructure in service of discipline and control.

Imagining un-subscription

This article began by interpreting the draconian frequency and intensity of Internet shutdowns in India as an indicator that they are growing increasingly routine and—for some communities—mundane, which paradoxically contradicts the Modi government's declared commitment to expanding connectivity in pursuit of creating a Digital India. Given Ali's (2016) suggestion that "computing is necessarily colonial insofar as it is modern" (18), this article brought together scholarship from Internet governance and e-governance in India to understand what Internet shutdowns reveal about an evolving digital citizenship regime. It identified m-governance—mobile governance—as an emerging technopolitical regime that is reconfiguring citizen–state relations by simultaneously investing in mobile telecommunications, essentializing mobile modes of citizen participation, while also rendering such access precarious through Internet shutdowns. This produces a form of digital citizenship in which citizen-state relations are mediated through—and, crucially, premised on access to—infrastructural digital technologies, and especially mobile Internet. This bifurcates the public along the faultline of mobile connectivity, casting suspicion on initiatives to close the digital divide as vehicles of predatory connectivity by subjecting targeted populations to routine disconnection.

These findings invite speculation about decolonial interventions; in other words, how can marginalized, peripheral communities "un-subscribe" from the network's disposition toward disconnectivity? On an individual level, previous work has documented how VPNs and decentralized networks using apps such as FireChat or Bridgefy (Parray, 2021; Poster, 2021; Shah, 2021) can be used to maintain connectivity in the face of a shutdown. However, these makeshift solutions do not address systemic problems. The network analysis in this article suggests that greater diversity among ISPs may complicate the dynamics of the network. For example, Freyburg and Garbe (2018) point to ownership models, suggesting that foreign telecommunications companies may be less likely to enact Internet shutdowns on suspect grounds. However, this option echoes previous programs by US-based Big Tech corporations to penetrate global South markets—such as the Free Basics program—that have been characterized as projects that perpetrate digital colonialism (Nothias, 2020). Ultimately, the most impactful interventions may come from the press and the public who have the collective power to ensure that Internet shutdowns do not reach the mundanity of load shedding.

More broadly, and especially outside the case of India, this article has illustrated some hazards of measuring the digital divide solely in terms of access to any form of Internet connectivity. Amid increasing adoption of digital and mobile governance practices, Internet shutdowns demonstrate that both stability and multiplicity of connectivities are crucial to ensuring that communities can enjoy both stable access to political and economic opportunities as well as broader notions of full digital citizenship.

Acknowledgments

Many thanks to j. Siguru Wahutu for his guidance and Noah D'Mello for feedback early in this project, and to the anonymous reviewers for their constructive engagement.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Rohan Grover https://orcid.org/0000-0002-9042-8259

Notes

1. In this article, "citizenship" refers to a relationship with the state, not necessarily to legal citizenship, which is itself under attack, particularly for Muslims; and "digital citizenship" refers to the technological mediation of citizenship in the digital age—especially, in the case of India, under Modi's Digital India regime.
2. Facebook's controversial Free Basics program offers free (zero-rated) access to a limited number of Internet services in the global South. Its launch in India—in partnership with Reliance Communications—inspired public backlash, which ended with TRAI banning the program in February 2016. For further discussion, see Nothias (2020) and Prasad (2018).
3. SFLC's Internet Shutdown Tracker can be found at https://internetshutdowns.in
4. Actor-network theory has been controversial for lacking—or actively avoiding—political analysis and for being overly descriptive. This article draws on ANT as one mode of analysis among many. In doing so, the aim is to not to ignore structural conditions or institutions, nor to excuse human actors from accountability for their actions, but rather to demonstrate how politics are stabilized relationally through and across sociotechnical and legal infrastructures with implications for citizen–state relations. This, inevitably, calls for political analysis, as described earlier through a framework of decolonial computing.
5. The Right to Information Act grants citizens the right to request information from public authorities.

References

Access Now (2019) The state of Internet shutdowns around the world: the 2018 #KeepItOn report. Available at: https://www.accessnow.org/wp-content/uploads/2019/07/KeepItOn-2018-Report.pdf

Access Now (2022) The return of digital authoritarianism: Internet shutdowns in 2021. Available at: https://www.accessnow.org/wp-content/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf

Akrich M (1992) The de-scription of technical objects. In: Bijker WE and Law J (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press: pp. 205–224.

Ali SM (2016) A brief introduction to decolonial computing. *XRDS: Crossroads, The ACM Magazine for Students* 22(4): 16–21.

Basu S (2021) Effective contact tracing for COVID-19 using mobile phones: an ethical analysis of the mandatory use of the Aarogya Setu application in India. *Cambridge Quarterly of Healthcare Ethics* 30(2): 262–271.

Baxter RM (2016) "Is this even legal?" Why is Narendra Modi in a Reliance Jio ad, ask Twitter users. *Scroll.in*, 2 September. Available at: https://scroll.in/article/815500/is-this-even-legal-what-is-modi-is-doing-in-a-reliance-jio-ad-ask-twitter-users

Bhardwaj S, Nayak N, Singh S, et al. (2020) Rising Internet shutdowns in India: a legal analysis. *Indian Journal of Law and Technology* 16(1): 122–158.

Bhatia J (2019) Crime in the air: spectrum markets and the telecommunications sector in India. In: Harriss-White B and Michelutti L (eds) *The Wild East*. London: UCL Press, pp. 140–167.

Caussat P (2017) Competing for public acquaintances. In: dela Rama M and Rowley C (eds) *The Changing Face of Corruption in the Asia Pacific*. London: Elsevier, pp. 209–219.

Chari M (2014) Riot-hit Vadodara may be on shaky legal ground in suspending telecom services. *Scroll.in*, 29 September. Available at: http://scroll.in/article/681322/riot-hit-vadodara-may-be-on-shaky-legal-ground-in-suspending-telecom-services

Chaudhuri B and König L (2018) The Aadhaar scheme: a cornerstone of a new citizenship regime in India? *Contemporary South Asia* 26(2): 127–142.

Cowen D (2020) Following the infrastructures of empire: notes on cities, settler colonialism, and method. *Urban Geography* 41(4): 469–486.

Dattani K (2021) "Goverentrepreneurism" for good governance: the case of Aadhaar and the India Stack. *Area* 52(2): 411–419.

Deccan Chronicle (2016) Modi's picture in full page Jio ads sparks controversy, Twitter goes crazy. Available at: http://www.deccanchronicle.com/nation/in-other-news/030916/modis-picture-in-full-page-jio-ads-sparks-controversy-twitter-goes-crazy.html

Deibert R, Palfrey J, Rohozinski R, et al. (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press.

DeNardis L (2012) Hidden levers of Internet control: an infrastructure-based theory of internet governance. *Information, Communication & Society* 15(5): 720–738.

Digital India (n.d.) Introduction. Ministry of Electronics and Information Technology. Available at: www.digitalindia.gov.in/content/introduction

Epstein D, Katzenbach C and Musiani F (2016) Doing Internet governance: practices, controversies, infrastructures, and institutions. *Internet Policy Review* 5(3): 10.14763/2016.3.435.

Financial Express (2016) Reliance Jio 4G launch: Mukesh Ambani dedicates Jio to PM Modi's Digital India vision. Available at: https://www.financialexpress.com/industry/reliance-jio-4g-launch-mukesh-ambani-dedicates-jio-to-pm-modis-digital-india-vision/363849/

Freyburg T and Garbe L (2018) Blocking the bottleneck: Internet shutdowns and ownership at election times in Sub-Saharan Africa. *International Journal of Communication* 12: 3896–3916.

Grover V (2021) Assessing India's legal framework on the right to peaceful assembly. International Center for Not-for-Profit Law. Available at: https://www.icnl.org/wp-content/uploads/India-freedom-of-assembly-report-2021-final.pdf

Gurumurthy A, Bharthur D and Chami N (2017) Voice or chatter? Making ICTs work for transformative citizen engagement. IT for Change. Available at: https://www.makingallvoices-count.org/publication/voice-chatter-making-icts-work-transformative-citizen-engagement/

Hecht G (2009) The Radiance of France: Nuclear Power and National Identity After World War II. Cambridge, MA: MIT Press.

Hindustan Times (2017) Reliance Jio, Paytm apologise for unauthorised use of PM Modi's photos in ads. Available at: https://www.hindustantimes.com/india-news/reliance-jio-paytm-have-apologised-for-using-pm-modi-s-photos-in-ads-says-govt/story-zqHqRkG4duZ7PF79g-t3usL.html

Howard PN, Agarwal SD and Hussain MM (2011) When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review* 14(3): 216–232.

IANS (2015) Modi stresses need for mobile governance. *The Hindu*, 30 January. Available at: https://www.thehindu.com/news/national/modi-stresses-need-for-mobile-governance/article6838050.ece.

Internet and Mobile Association of India (IAMAI) (2015) Internet in India 2015. Available at: https://cms.iamai.in/Content/ResearchPapers/a58218be-d7d9-4268-84e6-6c58aa4322ce.pdf

Internet and Mobile Association of India (IAMAI) (2019) India Internet 2019. Available at: https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf

Internet Freedom Foundation (IFF) (2021) Ahead of its visit to J&K, IFF apprised the Parliamentary Standing Committee on IT of repeated Internet shutdowns. Available at: https://internetfreedom.in/ahead-of-its-visit-to-j-k-iff-apprised-the-parliamentary-standing-committee-on-it-of-repeated-internet-shutdowns/

Jenson J (2007) The European Union's citizenship regime: creating norms and building practices. *Comparative European Politics* 5(1): 53–69.

Kaka N, Madgavkar A, Kshirsagar A, et al. (2019) Digital India: technology to transform a connected nation. McKinsey Global Institute. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation

Kathuria R, Kedia M, Varma G, et al. (2018) *The anatomy of an Internet blackout: measuring the economic impact of Internet shutdowns in India*. New Delhi, India: Indian Council for Research on International Economic Relations.

Kumar R (2021) *Police Matters: The Everyday State and Caste Politics in South India, 1900–1975*. Ithaca, NY: Cornell University Press.

Mamdani M (1996) *Citizen and Subject: Contemporary Africa and the Legacy of Late Colonialism*. Princeton, NJ: Princeton University Press.

Mare A (2020) State-ordered Internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication* 12: 4244–4263.

Mossberger K, Tolbert CJ and McNeal RS (2007) *Digital Citizenship: The Internet, Society, and Participation*. Cambridge: MIT Press.

Musiani F (2015) Practice, plurality, performativity, and plumbing: Internet governance research meets science and technology studies. *Science, Technology, & Human Values* 40(2): 272–286.

Musiani F, Cogburn DL, DeNardis L, et al. (eds) (2016) *The Turn to Infrastructure in Internet Governance*. New York: Palgrave Macmillan.

Nayak N (2018) *The legal disconnect: an analysis of India's Internet shutdown laws*. Working Paper 1/2018. New Delhi, India: Internet Freedom Foundation.

Nazmi S (2019) Why India shuts down the Internet more than any other democracy. *BBC*, 19 December. Available at: https://www.bbc.com/news/world-asia-india-50819905

Nothias T (2020) Access granted: Facebook's Free Basics in Africa. *Media, Culture & Society* 42(3): 329–348.

Pankaj J (2022) Mapping the rising Internet shutdowns in India since 2016. *The Wire*, 9 October. Available at: https://thewire.in/government/mapping-the-rising-internet-shutdowns-in-india-since-2016

Parray MI (2021) Choking the 'periphery': pride and prejudice in India's globalizing Internet imaginary. *Internet Histories* 5(3–4): 323–340.

Poster WR (2021) Striking by Telegram, avatar, and geotag: changing ICT landscapes of virtual protest in India. *International Journal of Communication* 23: 4360–4382.

Prasad R (2018) Ascendant India, digital India: how net neutrality advocates defeated Facebook's Free Basics. *Media, Culture & Society* 40(3): 415–431.

Press Trust of India (PTI) (2015) Digital India: PM Modi says India can play a big role in cyber security globally. *NDTV*, 2 July. Available at: https://www.ndtv.com/india-news/digital-india-pm-modi-says-india-can-play-a-big-role-in-cyber-security-globally-777319

Rao U and Nair V (2019) Aadhaar: governing with biometrics. *South Asia: Journal of South Asian Studies* 42(3): 469–481.

Roy PK (2019) Mobile data: why India has the world's cheapest. *BBC News*, 18 March. Available at: https://www.bbc.com/news/world-asia-india-47537201

Ruijgrok K (2022) The authoritarian practice of issuing Internet shutdowns in India: the Bharatiya Janata Party's direct and indirect responsibility. *Democratization* 29(4): 611–633.

Schia NN (2018) The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly* 39(5): 821–837.

Shah N (2021) (Dis)information blackouts: politics and practices of Internet shutdowns. *International Journal of Communication*: 15: 2693–2709.

Sharma S and Singh S (2008) Gandhian strategies for democratic decentralisation and development: dimensions on rural development, gram swaraj, and Sarvodaya. *The Indian Journal of Political Science* 69(4): 727–744.

Shu C (2015) India will have 500 million internet users by 2017, says new report. *TechCrunch*, 21 July. Available at: https://techcrunch.com/2015/07/21/india-internet-growth/

Singh M (2020a) Facebook invests $5.7B in India's Reliance Jio Platforms. *TechCrunch*, 21 April. Available at: https://techcrunch.com/2020/04/21/facebook-reliance-jio/

Singh M (2020b) Google invests $4.5 billion in India's Reliance Jio Platforms. *TechCrunch*, 15 July. Available at: https://techcrunch.com/2020/07/15/google-invests-4-5-billion-in-indias-reliance-jio-platforms/

Sinha A (2019) India's porous state. In: Jaffrelot C, Kohli A and Murali K (eds) *Business and Politics in India*. Oxford: Oxford University Press, pp. 50–92.

SK C and Lakshané R (2018) *Of sieges and shutdowns*. The Bachchao Project. Available at: https://thebachchaoproject.org/of-sieges-and-shutdowns/.

Software Freedom Law Center (SFLC) (2018) Second appeal to the RTI application revealed procedural lapses. Available at: https://sflc.in/second-appeal-rti-application-revealed-procedural-lapses-only-11-review-committee-meetings-despite

Software Freedom Law Center (SFLC) (2020) Internet shutdowns in India since 2012 (Data set). Available at: https://internetshutdowns.in/

Spikes Asia (n.d.) Jio Phone - passport to Republic of Digital India. Available at: https://www2.spikes.asia/winners/2018/innovation/entry.cfm?entryid=2709&award=101

Subramanian R (2020) Tracing India's (cyber) security history from colonial times to the present: has anything changed? *IEEE Annals of the History of Computing* 42(4): 71–83.

Telecom Regulatory Authority of India (TRAI) (2020) Telecom subscription data as on 30th December, 2019. Available at: https://www.trai.gov.in/sites/default/files/PR_No.17of2020_0.pdf

Thakurta PG and Kaushal A (2010) Underbelly of the great Indian telecom revolution. *Economic and Political Weekly* 45(49): 49–55.

Thakurta PG, Ghosh S and Chaudhuri J (2014) *Gas Wars: Crony Capitalism and the Ambanis*. New Delhi, India.

Vargas-Leon P (2016) Tracking internet shutdown practices: democracies and hybrid regimes. In: Musiani F, Cogburn DL, DeNardis L, et al. (eds) *The Turn to Infrastructure in Internet Governance*. New York: Palgrave Macmillan, pp. 167–188.

Wagner B (2018) Understanding Internet shutdowns: a case study from Pakistan. *International Journal of Communication* 12: 3917–3938.

Wani JI (2022) Regulating hooligans and Mawaalis: collective action and the politics of public order in late colonial India. *South Asia: Journal of South Asian Studies* 45(1): 19–35.

Author biography

Rohan Grover is a PhD student at the Annenberg School for Communication and Journalism at the University of Southern California. His research focuses on technology policy, critical data studies, and political communication.