International Journal of Communication 15(2021), 2693–2709 1932–8036/20210005

(Dis)information Blackouts: Politics and Practices of Internet Shutdowns

NISHANT SHAH
ArtEZ University of the Arts, The Netherlands

Various emerging digital information societies like India exercise Internet shutdowns and information blackouts regularly as a way of dealing with different kinds of crises. These blackouts are justified as countering the misinformation cycles that amplify (dis)information that we have come to characterize as "fake news." An immersive ethnography during an Internet shutdowns in India revealed these blackouts are neither absolute nor foolproof because blackouts have multiple back doors that allow different kinds of information to flow through networked and social negotiations. I argue that Internet shutdowns need to be seen as specific exercises of geopolitical and sovereign power and read as performative because they are both inefficient and ineffective in achieving information blackouts. Making a distinction between misinformation and disinformation, I show how these Internet shutdowns do not stop the circulation of fake news but, as infrastructural tools, they enable state (dis)information and propaganda to spread without resistance and thus become potent tools in curbing protests and rightful critique of authoritarian practices.

Keywords: disinformation, Internet blackouts, freedom of speech, Internet governance

In 2018, India topped the notorious list of countries with the highest number of documented Internet shutdowns, with 134 instances in that year (Software Freedom Law Centre [SFLC], 2019). India has been building itself up as a digital hub with national campaigns like "Digital India" and "Make in India,"[1] both of which predicate the rise of digital making and connectivity as a way of building wealth and prosperity for the country. It was ironic that the government, which has been positioning digital extensions as a way to address problems ranging from wealth inequity to spiraling unemployment, decided on frequent Internet shutdowns as a desired tool of governance. These numbers have only continued to intensify in the following years, appearing as a one-stop solution to several different kinds of crises. Shutdowns have been ordered as a response to the *WhatsApp Lynchmobs*, comprised of right-wing Hindu cow vigilantes who attacked members of the Muslim minority in the country (Burgess, 2018). They were implemented in the service of national security, noticeably leading to the longest-standing Internet shutdown in the state of Jammu and

Nishant Shah: itsnishant@gmail.com
Date submitted: 2019-11-21

[1] Revati Prasad (2018), in her analysis of Facebook's Free Basics service in India, argues quite convincingly that the mantle of "Digital India" has often been used to override consumer and citizen rights in the interest of developmental aspiration.

Kashmir, which was bifurcated into two Union Territories after the abrogation of Section 370 of the Indian constitution (Schultz & Yasir, 2020). They were instated to deter public protests and participation during the nationwide protests against the Citizenship Amendment Bill and the National Registry of Citizenships aimed at delegitimizing migrant and minority communities (Netblocks, 2019). It was deployed to curb the student protests across the country, asking for freedom of academic speech and expression during clampdowns on public intellectuals in universities (Singh, 2019), and it was even mobilized during the mandatory lockdown in the face of the COVID-19 measures.

In almost all of these cases, the government at the central and the state levels cited misinformation, fake news, rumor, and panic-mongering as the problems that elicited the Internet shutdown as a response.[2] Given the lack of accountability on social media platforms (Van Dijck & Poell, 2013) and the encrypted nature of closed online communication tools—the loss of control on information content—the shutting down of the infrastructure of communication seemed to be the only available option. Although all governments do have reasonable rights to take control of these infrastructures[3] (International Telecommunication Union [ITU], 2001) and to control them in protection of their people and security of their territories, the Human Rights Watch World Report (Roth, 2020) explains in detail that these shutdowns as a way of regulation and governance are both ineffectual and counterproductive.

In an interview with *Politico*, Subrahmanyam Jaishankar, the minister of External Affairs, accepted that Internet shutdowns were problematic, but he couldn't find a way out where we can "cut off communications between the terrorists and their masters on the one hand, but keep the Internet open for other people" (Brown & Oliver, 2019, para. 21). This idea that Internet shutdowns establish effective information blackouts is echoed multiple times by the Indian government as a justification for the shutdown.

---

[2] This article is particularly interested in exploring this coupling of Internet shutdowns and information blackouts. As Mishi Choudhary (2019), a lawyer and founder of the Software Freedom Law Centre India, very precisely points out that

> governments have this mistaken idea that the way to shut down the Internet generation is to shut down the Internet. The government of India cannot push for Digital India on one hand use the kill switch to turn it off with the other. (para. 22)

[3] Articles 34 and 35 of the Constitution of the ITU, for which India is a signatory, provide specific clauses for the shutting down of telecommunication networks and infrastructure. Article 34 declares that "Member States reserve the right to stop, in accordance with their national law, the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its law" and also reserves the right of the member states to "cut off, in accordance with their national law, any other private telecommunications" (p. 98) on grounds of security of state of public order or decency. Similarly, Article 35 bestows the right on each member state to "suspend the international telecommunication service, either generally or only for certain relations/and or for certain kinds of correspondence" (p. 98) given the nature of the situation. However, the constitution does not condone complete shutdowns and suspension of connection in entire regions, and these Internet shutdowns can be seen as directly violating the charter of the ITU.

V. K. Saraswat, a member of the NITI Aayog[4] team, controversially defended Internet shutdowns as inconsequential. "What difference does it make if there's no Internet there? What do you watch on Internet there? What e-tailing is happening there? Besides watching dirty films, you do nothing there" (The Press Trust of India [PTI], 2019, para. 3), he ranted at a press conference. He defended the shutdown by insisting that the shutdown was a way of information blackout: "If Article 370 had to be removed, and if Kashmir had to be taken forward, we knew that there were elements which would misuse this kind of information in a manner that will affect the law and order situation" (PTI, 2019, para. 5). In a landmark case by the SLFC against the government of West Bengal, when a suspension of Internet services was ordered to curb dissent, the court ruled that such suspensions made possible under the "Temporary Suspension of Telecom Services (Public Emergency or Public Safety)" cannot "trivialize the shutdown" to suit the state's purpose and, in fact, is ineffective in the control of information (Jalan, 2020, para. 4).

In the state of shutdown, the mechanisms of legitimized surveillance also disappear, leading to a lack of control in the affected regions. Moreover, it has often been seen that the blocking of material and hardware infrastructure (Open Net Initiative, 2007) and modes of access (Mozilla Foundation, 2019) only open up new modes of information flow that continue to bypass these shutdowns by creating new streams and forms of blended connectivity. Though governments shutting down the Internet often do it to exercise information blackouts, I will seek to argue that the one does not lead to the other. In this article, I draw from a survey of 1,000 in-person responses, gathered during an Internet shutdown in the city of Ahmedabad, Gujarat, in 2015, to show how the shutdown is neither absolute nor foolproof. Looking at the "leaks" and inefficiency of infrastructure implementation, it shows how people find new ways of navigating through and building information ecosystems. It establishes that, far from countering misinformation and fake news, shutdowns both intensify and amplify malicious and harmful information by removing tools of verification and fact-checking from the individual users. I further argue, drawing from the anecdotal evidence of information negotiation and flow during other shutdowns, that this performance is not just a show of power but also an infrastructural tool that allows for the state to gain monopoly over information and to propagate (dis)information by taking control of the communication infrastructure. Drawing on the introduction to this special issue by Hoyng, the excessive forces of information and affect during a shutdown are not purely liminal vis-a-vis state power but manifest less expectable coalescence between digital infrastructure and state power through repression of dissent. I conclude by offering some observations about how Internet shutdowns are not information blackouts but (dis)information blackouts, and how they avoid the accountability and transparency established in anticensorship and intermediary liability law, to dissuade and make invisible the voices of protest and dissent.

Internet Shutdown ≠ Information Blackout

In 2015, in the city of Ahmedabad, in Gujarat, India, an Internet shutdown was announced when Hardik Patel, a 22-year-old activist-politician called for a "Maha Kranti Rally" (Epic Evolution March) through

[4] NITI Aayog is the National Institution for Transforming India, a policy think tank of the Government of India, created to achieve sustainable development goals with interstate cooperation. It is one of the innovation and development bodies of the government with specific input and championing of digital solutions and technologies.

the organization Patidar Anamat Andolan Samiti (PAAS). This peaceful march for the inclusion of the community of Patidars in the category of Other Backward Class (OBC) that grants them benefits of affirmative action in education and employment (PTI, 2015), was expected to have 500,000 members of the community coming together on the massive Gujarati Mineral Development Corporation (GMDC) grounds of the city (Express News Service, 2015). After a few hours of spirited speeches, the demonstrators marched to the office of the district collector, effectively engulfing the entire city and bringing everything to a standstill (Langa, 2015). Patel, who ended his speech by announcing an indeterminate hunger strike until his voice was officially heard by the chief minister of the state—along with some of the key organizers—was arrested because they did not have adequate permissions to stay on the grounds. The news of his arrest agitated the otherwise loud-but-peaceful crowd into acts of mob violence, leading to ten deaths, vandalism, and destruction of property across the state (Shaikh, 2015). The state government of Gujarat also imposed physical curfews in a few cities, accompanied by a state-wide shutdown of the Internet (The Hindu, 2015) to thus stop physical movement of people and digital movement of information in an attempt to stop rumors and people gathering.

The shutdown lasted for five days, with intermittent relaxation and clampdown on information transfer, after the political negotiations between the PAAS and the chief minister found fruitful ways forward. Immediately after the shutdown, with a team of six researchers, we conducted an in-person and telephonic survey of 1,000 respondents across the city to get a snapshot of how people engaged, navigated, and negotiated with the shutdown.[5] The larger project, which paralleled similar studies in other South Asian countries, was particularly interested in thinking through the state of freedom of speech and expression and the shutting down of civic spaces. It resulted in a policy brief after a five-year-long exploration of the mechanics of Internet shutdowns in different parts of the world. However, some other significant responses emerged from the surveys. For this article, I draw from the data gathered in the research in India, but it has many resonances with the findings in the other countries. I am particularly focusing on the responses that revealed a few axiomatic truths about the material and practical nature of such Internet shutdowns that helped make a decoupling between Internet shutdowns and information blackouts.

Shutdowns Are Leaky

One of the most evocative observations that emerged in the responses was that digital shutdowns are leaky. They are not uniform, are difficult to implement in a multi-intermediary society, and have loopholes and back doors that are both human and technological and that allow for flow of information even in the face of a regulatory shutdown. A significant number of respondents showed how they did not experience the shutdown, but actually heard about the shutdown from their social media streams. "I was online and then I heard that the Internet has been shut down an hour ago, but I was still online," (Interviewee #372) one of them quipped. The initial ban was on only mobile data and was extended later to Wi-Fi networks as well.

[5] This survey was initiated through the Centre for Internet and Human Rights in Berlin, in close collaboration and with support from Ben Wagner. The on-the-ground collaborators were Prof. Dipti Kulkarni at MICA University in Ahmedabad, who worked with a team of five master's students—Devendra Dave, Vaibhavi Joshi, Vani Chandra, Aditya Saraf, and Lagan Mongia—who tabulated the data and helped mobilize the quick response to capture the impressions of people while they were still experiencing or had just experienced the disconnection in the city.

However, given the nature of broadband operation in India, with the broadband connection tied to landline telephony and many still using dial-up connections, there was connectivity. There were others who also commented on how some of their family members who had different service providers still had access to digital information, even as some of the others went down.

Alexander Galloway (2004), in his material analysis of digital protocols, had suggested that the intention of digital regulation and the practice of digital transactions are not naturally bound. Protocols engineered within the systems are difficult to overturn merely by regulatory mechanisms that seek to control them from the outside. Wendy Chun (2016), in her positing of "habitual new media" (p. 1), gives a parallel example by looking at traffic—circulation of data—as the only currency and lifeline of digital computation networks. In her postulation, the Internet is "a series of poorly gated communities" that lead to a condition where "YOU are constantly betrayed by people who 'like YOU' and who are algorithmically determined to be 'like YOU'" (Chun, 2016, p. 16). Chun's critique of leaky networks is intended to warn us against the corporations that continually bleed data into different sets and streams, creating user profiles and selling it for profits. However, this leakiness also seems to work in the face of mandated Internet shutdowns, where information continues to leak through different practices.

Many of the younger respondents in the surveys also had multiple technological hacks into staying online. Respondents pointed toward "Psiphon"—the free and open-sourced Internet censorship circumvention tool that uses a combination of secure communication and obfuscation technologies (Interviewees #252, #384, #403). Several of them used GPS spoofing apps and VPN networks that changed their locations outside of the shutdown area and brought data to their phones (Interviewees #26, #45, #196, #490, #688). There was a sizeable group of respondents who showed us peer-to-peer mesh that they implemented using apps like Bridgefy and FireChat to create Local Area Networks (Interviewees #12, #58, #128, #144, #349, #688, #787, #792, #842, #912, #934, #967) or what Duncan Watts (2016) calls *small worlds* to remain connected within their communities. Many of them cited the lessons learned during the so-called Arab Spring and the revolutions in Hong Kong (Lakshmanan, 2019), where they had already seen these apps and hacks in action.

It was important for us to realize that the announcement of an Internet shutdown is not the same as implementing it. The infrastructure in free markets is not easily controlled by the governments, and the differing protocols, policies, and politics of the service providers often create a patchy shutdown where information trickles and then immediately gets virally shared to reach different nodes that might be offline but not disconnected.

Technological Shutdowns Have Human Workarounds

Perhaps even more telling in these responses was the idea of collective Internet resources. Although the one-device-per-person logic often individualizes online access, the on-the-ground reality is not that clean. Multiple households use mixed access devices with different service providers chosen based on tariffs and plans. People are not only used to sharing devices but also common passwords and access points in families, friend-groups, and even in some neighborhoods. Hence, when the first shutdowns happened, those who still had access to the Internet started creating mobile hotspots for others to receive information and to stay connected. Some pointed out that the "Internet dongle"—a mobile data connection hotspot—was operational

in the face of both broadband and phone-based Internet shutdown, and thus these portable hotspots got easily shared and even travelled across the city in some instances (Interviewees #9, #27, #45, #89, #92, #103, #105, #112, #235, #237, #265, #451, #558, #572, #602, #612, #677, #724, #781, #793, #805, # 912, #915, #934, #968). There was a steady gathering of information about which service providers were still offering data and what kind of apps they were offering. As one of the respondents gleefully pointed out, "there were a lot of service providers like AirTel and Reliance which did not block WhatsApp, but they blocked web access" (Interviewee #84). From there, it was only a matter of time to start piracy, sharing of information, and entertainment materials through these digital messaging services.

In my other work on piracy and pornography, and particularly on queer porn, which remained outlawed in India until recently, I have presented the idea of a *pervert-to-pervert* network. Particularly looking at how different communities in the penumbra of the law find different forms of information exchange and sharing, I have argued that for many communities, the delegitimization of their desire and penalization of their identities mean that they have always been in a state of semishutdown. Given the amount of regulation that has emerged around piracy and pornography in the Indian context, it is helpful to make the connections between these contexts of information sharing that have always been restrained or punished; and yet, they continue to find persistent ways of connecting that are part technological and part human. Kara Keeling (2014) calls this the "queer OS":

> It understands *queer* as naming an orientation toward various and shifting aspects of existing reality and the social norms they govern, such that it makes available pressing questions about, eccentric and/or unexpected relationships in, and possibly alternatives to those social norms. (Keeling, 2014, p. 152)

Anita Say Chan's (2014) explorations of building digital infrastructure on the margins also reinforces this idea. Looking at universalist constructions of digital knowledge-based systems, Chan shows that the dissemination of supposedly universal conceptions of law—in her case, intellectual property law—does not cohere with the realities and concerns of most of the world's population. In her exploration of communities with alternative knowledge management regimes in Peru, Chan offers the conception of a *polyvocal network* of activists working within and through alternative forms of digital knowledge and network management. These are no longer controlled by the "dominant logics of software innovation and the established practices of closed, proprietary commercial development that most IT product markets relied on" (Chan, 2014, p. 117). Chan reads these acts as resistance to the myth of the information society and opens up the messiness of humans in their engagement with technological practices.

The respondents in this survey are not activists, and they would not particularly claim to be hackers. Many of them confessed to not having much technology savvy to circumvent such a disconnection but also showed willingness to learn more about this. At the same time, they had already extrapolated from other contexts inside and out of India and started looking at human workarounds that depended on collective knowledge, shared resources, and the confidence of finding a hack to resist the shutting down of their digital infrastructure. Their default aesthetic and mode of engagement in digital networked practices is the FOAF (friend of a friend) reliance that naturalizes this pooling together of information and sharing of resources that was not imagined in the regulatory shutdown.

Digital Networks Are Greater Than Interface Interactions

Although some of the most prominent focus during the shutdowns is on everyday social media practices of the Internet, the survey clearly showed that the true costs of the shutdown, beyond freedom of speech and expression, are in the delivery of critical services. With the unexpected shutdown, there was a sudden halt on banking transactions, as people increasingly have depended on e-banking and mobile payments in India in the last few years. It was surprising for respondents to realize that not only do they not have enough physical cash, but their digital money and credit cards would also not work because of a lack of Internet connectivity in places of commerce. Some of the respondents clearly pointed out how they had difficulty accessing medical reports, financial services, and customer data to perform their work and also to provide critical services. The unforeseen and overlooked cost of Internet shutdowns is often in the denial of service that emerges from most organizations and individuals never anticipating such disconnection, and hence not preparing for contingencies to continue working with their everyday practices.

From the second day of the shutdown, it became apparent that, while the individual user still depended on mobile telephony for Internet access—the rates of broadband penetration remain significantly low because of a lack of infrastructure and affordability—business and workspaces needed digital access. Thus, certain connections were restored, and people quickly realized that the Internet at work is still Internet that they can use for other things. Respondents reported that they started going to their offices early or staying late to consume and share non–work-related information through these connections. "It is perhaps unethical but I just came to office early and downloaded things to see at home in the evening," one respondent said (Interviewee #586). Another pointed out that arrangements were made with a "neighborhood shop" (Interviewee #204) where the individual could siphon Internet for personal use. A few also admitted that they knew the local lines persons from the service providers and, by using personal influence, could just get their connection reinstated without going through any bureaucracy or administration (Interviewee #334, #392, #468, #553, #684, #726).

The informal nature of these "pirate modernities" (Sundaram, 2010, p. 23) that mark the landscape of information infrastructure in India, coupled with the growing dependence of everyday life on digital connectivity, meant that despite the blanket shutting down of the Internet, there were pockets of connectivity necessitated by the use of the Internet beyond just spaces of misinformation and social engagement. However, these "essential spaces of business and commerce" (Sundaram, 2010, p. 56) became gateways to opening up the floodgates of information flow, which ensured a steady stream of messaging, viral videos, and news spreading across the city.

Information in Mixed-Media Ecologies

Both during the blackout and after, even those who thought that the Internet shutdown was a necessary, albeit sometimes performative, step in which the government can be seen doing something in the face of crises agreed unanimously that the Internet was not the only information stream. Almost all respondents agreed that the shutting down of the Internet had no effect on their reception and consumption of news and, in many cases, unsubstantiated reports. As one of them very clearly stated,

> All that was happening in the city was shown in the televisions. Newspapers also gave the information. There were pictures of buses being set on fire and chaos. So the rumors were still not curbed. So I believe that disconnection is not the solution to such disturbances in the society. (Interviewee #173)

Similarly, most respondents agreed that there was no connection among the actual physical riots, acts of vandalism, and the digital disconnection. "Disconnection is not a solution for providing a safe environment to the people . . . riots should be controlled, not the flow of information" remained a repeated trope across many responses (Interviewee #621). As one respondent echoed many other voices, "disconnecting the Internet also gives police a chance to behave improperly as people cannot report live incidents" (Interviewee #38). The verdict was clear that the Internet shutdown was misplaced responsibility and guilt, where the government, unable to censor the demands of the protestors and not allowed to violate their constitutional rights for protest, could not make any physical actions. Although the curfew on movement in some parts of the city was effective after the acts of vandalism and violence, the only space where the government could perform control and power was on the digital spaces. There, too, in the complex intermediary liability framework (Abraham, 2019), where content cannot be easily removed or erased, the only brute-force solution was an Internet shutdown.

However, the shutdown did not curb the flow of information. If anything, it amplified distrust and created conditions of circulation where verification and fact-checking became impossible. People received rumors on phone calls and text messages. News spread from home to home across neighborhoods. Other relatives and friends in different parts of India, who were getting news from other sources, started relaying half-baked news about widespread vandalism and destruction to their connections back in the shutdown zone. However, those who were stuck in the shutdown with restricted access had no means of actually verifying and evaluating the veracity of this information. Ironically, the access to information through other means and not having the capacity to fact-check it using digital tools meant that the Internet shutdown succeeded in increasing the spread of misinformation and reduced the agency to counteract it.

Shutting down the Internet was not the same as blacking out information. Instead, it created a small bubble of information engagement and exchange and reduced the users into mere recipients of information that they shared and consumed without having the tool to verify and value it. Contrary to the government's claims that the Internet shutdown blacked out information and thus led to the feeling of safety and security, it is obvious even from this symptomatic survey that an Internet shutdown in its patchy, fragmented, uneven, and human implementation is never enough to stop the information flow. Instead, it allows for rampant circulation of information that does make its way into the closed networks, creating easy conditions for misinformation and fake news to proliferate.

Misinformation/(Dis)information

If the inefficacy of Internet shutdowns to curb information circulation is so evident, the logical question remains as to why governments continue to engage in this infrastructure closure during times of crises. I propose that one way of understanding the relationship between Internet shutdowns and information blackouts is to make a distinction between misinformation and disinformation. Though semantically similar, the two refer to specific kinds of verification and authorization processes.

Misinformation is false information provided to willfully deceive or deliberately mislead the recipient of the information. Misinformation, thus, is a lie or fake news, and, on verification, can be easily debunked and delegitimized. It is in the nature of misinformation that, within itself, it contains falsehood that can easily be detected by human experience, contextual mapping, source verification, and collective fact-checking. Take the case of the WhatsApp lynch mobs that India witnessed in the last few years, where unbridled and unverified information inserted into close-loop circles led to impromptu mobs organizing to participate in random acts of violence.

In one of the most well-documented cases, Mohammad Azam, a software engineer working with Google, had gone on a pleasure ride in his car with a relative and a friend in the district of Bidar. One of the members of the group, who was visiting from Qatar, had a box of chocolates with him. At a stop where they were stretching their legs, he saw a group of schoolchildren passing by and looking at them, and he offered to share some chocolates (Indo-Asian News Service [IANS], 2018).

Unbeknown to them, they had entered a region that was bristling with WhatsApp videos warning of child abductors, sharing videos without provenance. Even though there had been no cases of kidnapping, the communities in the villages were firmly convinced that multiple children had gone missing. The videos were shared in a closed cybernetic loop among people who had already convinced themselves of the news even before they received the videos. The conspiracy theories had already taken hold of the public imagination, so the blurry, unverified videos were never fact-checked, and, like rumor or information without signature, they spread across the communities.

Hence, when somebody reported that these men stopping in the village were offering chocolates to children, a mob quickly assembled. They started abusing the group, who got into the car and fled. However, the information of their arrival had passed much faster than their travel, and so in the neighboring village of Murki, they were blocked by an angry mob that dragged out the occupants and started beating them with sticks and stones. By the time the police came to stop them, Azam had already died on the spot, whereas others sustained critical injuries and were taken to the hospital (Reuters, 2018).

Even though the victims bore all the markings of affluence and middle-class respectability, the mob insisted on misreading them as kidnappers. In the police reports, they talked about how all their explanations, providing of identification, and trying to prove their innocence had fallen on deaf ears. In the testimonies of bystanders, it was shown that the videos without proof were used as verification tools to frame the victims. There were people who were playing the videos on their screens and using those images to seek resemblance with the victims, using this fake information to ascribe real identities.

Misinformation like this, however, is easy to disprove and discredit. On mass messaging platforms like WhatsApp, there are already algorithmic practices to show forwarded messages as originating elsewhere and a machine learning analysis that flags potentially dangerous content. Twitter famously started flagging potentially fake news by verifying source, content, and metadata, whereas Facebook and Instagram have deployed information cleaning crews that remove suspicious and reported content that violates the terms of service—misinformation and deliberate falsehood being two of the key criteria. Similarly, fact-checking websites, specific hashtags, and discussion forums also mark misinformation clearly and quickly and can help in stopping its flow.

Disconnection interventions in the form of Internet shutdowns are useful to slow down the spread of misinformation, use reliable sources to fact-check and recognize through pattern detection potentially fake and abusive information, and thus prevent the dangerous consequences of its spreading. Internet shutdowns poke holes in the logical closed-loop networks of this information circulation. As Maria Manzano (1996) argues, within the first and second order of logic, "we will never find a strongly complete deductive calculus . . . (because) compactness, which could be proven from strong completeness, fails" (p. 2). She draws from the history of logic to remind us that "a complete calculus can never be obtained" (pp. 5–6), and so computational networks that promise stability and validity of an information set can hold on to the *truthiness* only within the closed system of that network. Bringing in external verification tools immediately shows the fallacy of the information, and it can be quickly identified as misinformation.

Mathematician and data scientist Cathy O'Neil (2016), in *Weapons of Math Destruction*, shows how digital information in a computational network gets mapped in a matrix of data, links, indices, and algorithms. This particular set of network transactions ensures that the information is continually in circulation within a network and is stopped only when an external measure or protocol is applied to it. O'Neil (2016) explains that data, once generated in a computational network, is modified and revaluated to form abstractions and specifications through internal and external links. Links are not just the relationality between these data sets but also the edges of the network that make new and unexpected connections with external data and information. This extension of the network is material as well as ideological. The act of introducing counterdata or verification protocols immediately collapses the equilibrium of this network and stops the perpetuation and circulation of this information.

Thus, misinformation, which is information that has just not been verified yet, can effectively be controlled by Internet shutdowns that slow down its circulation and give space for new information and indexes of relational links to be introduced into the network to stop the spread. Even if the Internet shutdown is patchy and not uniform, it does provide an impediment to the free flow of rumors by introducing provenance, testimonies, and pattern recognition from alternative and reliable sources to discredit and disprove the information. It also puts a pause on easy access to fake news and information, often engineered by troll bots and human fake-news armies hired by malicious interest groups to circulate this content. Eventually, the misinformation can be stopped by testing it against structures of veracity and proving it wrong because the fakeness and deception are inherent in the very nature of this information.

Contrary to misinformation, disinformation does not subject itself to easy scrutiny and fact-checking. Disinformation specifically refers to false information intended to mislead, specifically propaganda issued by governments to rival powers or to the public. Disinformation is an act of secrecy and manipulation, where the provenance, authority, and authorship of the information is not under question. It is not the introduction of fake information in a data stream; it is the introduction of fake information as reliable and truthful, supported by institutional logics of verification, and thus spread with legitimacy that is difficult to discredit.

Although disinformation cycles and a state's manipulation and hiding of information in a post-Snowden world does not surprise us, its insidious nature and authoritative circulation is quite alarming. Take the extremely charged case of Kanhaiya Kumar, a young political activist in India. In February of 2016, Kumar, along with other former members of the Democratic Students Union, organized a protest at the Jawaharlal

Nehru University campus to oppose the capital punishment handed to Afzal Guru, who was convicted of terrorist charges for an attack on the Indian Parliament in 2001 (Chatterjee, 2016). The protest ended in clashes with the Hindu nationalist student union Akhil Bhartiya Vidyarthi Parishad, and videos of the clashes and the event went viral. Particular among these witness videos was a set of clips circulated by the conservative Indian news channel Zee News that purportedly showed Kumar and his fellow protestors shouting "anti-India" slogans. These clips became the basis for Kumar to be arrested on charges of sedition.

It required forensic digital investigations for the legal courts to acquit Kumar as the reports showed that the "footage had been tampered with" (Hafeez, 2016, para. 17). Further scrutiny revealed that the audio that was inserted into the clips was from a different group of people assembled there and overlaid on the video clips of Kumar and his allies. Their protest performance, asking for the death of social evils like caste and communalism, easily got doctored into evidence of seditious sentiments (Kanwal, 2016).

The problem with these doctored videos was that they could not be easily disproved by an algorithmic pattern analysis that could question their veracity, provenance, source of origin, or the hermeneutic content. Engineered by militant state parties, condoned by a national TV channel that presented them as verified truth, and then quickly made viral to produce truth by repetition, the videos were proven as authoritative proof of the state of affairs. Neither the testimonies of Kumar nor the evidence of many other neutral witnesses, including other media reporters who insisted that this video was not "true," could counteract the authority with which this disinformation was presented.

The falsehood in these videos was not contained in the text or on the dubious nature of the source that was spreading them, but in the intention and the coded manipulation. All individual or human attempts at disproving or denying them would fall flat because the truth value of the video was supported by large institutional structures that were the arbitrators of truth in checking the veracity of information. The only way by which this material could be disproved was by a legal process that fought code with code, digital manipulation with reverse engineering, and thus produced a counteraction that deemed these videos as misinformation. There was an elaborate process of gathering alternative data sets, creating simulations of manipulation, and identifying the malicious code, which was possible because there were alternative videos and testimonies of that particular event available. The reason why this disinformation could be labeled as misinformation was because of the polyvocal testimonies and data streams that presented an alternative picture. In the absence of these narratives, the only available information would have been these doctored videos, which were both authored and authorized by the state and its apparatus as legitimate truths.

For disinformation to survive, it would seem, an Internet shutdown is the best condition. As we have seen earlier, even in an Internet shutdown, information flows. However, with impeded access, blocked resources, and controlled flow of information, the disinformation that comes with political and legal authority flows unimpeded. Internet shutdowns are a way by which the state foregrounds itself as the central source and verifier of information, and thus specifically shaped information, manipulated data sets, and propaganda can be easily transferred and circulated unchallenged amid an Internet shutdown. As has been seen in multiple instances during the Internet shutdown, the state information channels are not blocked, and access remains open. However, the state-sanctioned outlets become the gatekeepers of information flow, thus controlling the

narrative and intimidating free speech, which might be considered seditious or dangerous and thus erased rather than censored.

(Dis)information Blackouts: Rights and Resistance

Ashish Rajadhyaksha (2011), in his formulation of the *Cultural Last Mile* (p. 12), shows that this infrastructural gatekeeping does not happen merely in times of crises, but the state continues to position itself as the superintermediary that would oversee the physical and spectrum networking for mobile telephones in the country. A private telecom operator might have mobile service licenses in two adjacent states, but it was not allowed to interconnect its networks. The traffic from one network had to be routed through the Department of Telecommunications, which would carry it through a physical distance to the second network of the same private telecom operator, charging it for this operation. Rajadhyaksha (2011) writes,

> The private operators—the new messiahs of the Last mile—had to go *physically* all the way round the blockage (and also) . . . had to make something of a *discursive* detour . . . around a gigantic barrier in the shape of the Department of Telecommunications. (p. 70)

Rolien Hoyng and Murat Es (2017), in their analysis of the blockage-censorship nexus in Turkey, observe that "these instances of censorship through blockage and disconnection are inscribed by sovereign decision and moral authority" (p. 4224). In a more tumultuous crisis of national sovereignty with the reformulation of Jammu and Kashmir (J&K) as Union Territories, removing its constitutional statehood, the Indian government implemented the longest shutdown of 213 days (August 4, 2019–March 4, 2020) that a democratic country has ever done. During this period, fraught with tension with Pakistan and military presence in the region, it was deemed necessary by the government to suspend Internet access to all the people living in J&K. Social media was agog with commentary around this—with nationalists rejoicing in taking Kashmir back and liberalists and constitutionalists appalled at the abrogation of a constitutional provision, the voices from within the region remaining absent from the conversations.

The absence of the populations directly affected from this disconnection is not new because the region has suffered continued disconnections to curb antinational sentiments and expressions. However, this prolonged ban, where only the story told by the Indian government could travel across the country, and within the disconnected region, was new. Naseer Ganai (2020) cites Haroon Rashid Shah, the editor of the Urdu daily *Nida-i-Mashriq*, as saying, "Internet ban is the ban on newspapers." Bashir Manzar, the editor of an English daily *Kashmir Images*, wryly mentioned, "I can tell you what is happening in New York, but I don't know what is happening in Sapore," a town about 50 kilometers away from where he lives in Srinagar (Ganai, 2020, para. 3). The Human Rights Watch reports cite a citizen saying, "in effect, the government places all of us in prison," and the only voice that was being heard internally and externally was the voice of the government and the story that they had to tell (Ganai, 2020, para. 6).

Prime Minister Narendra Modi reached out to the people of Jammu and Kashmir and Ladakh via Twitter the day after the abrogation of Article 370, ironically, after Internet access was already suspended in the region (Sircar & Sachdev, 2019). The authorities continue to insist that the Internet shutdown saves lives (HT Correspondent, 2020) and throughout the lockdown kept putting forward a picture of peaceful transition

and rejoicing populations standing in support of the government's decision. However, as Shahnaz Bashir (2019) writes in *Time*, the government's insistence that "All is well in Kashmir" belies the reality of living in a military state without any access to make your stories heard (para. 14). In a poignant opinion editorial in *The Indian Express*, Jaleel, Masood, and Akhzer (2019) write, "Sure, the Valley has seen many a strike, many a curfew, but this time there's no escaping the difference—with neighbourhood locked away from each other, too, Kashmir has been turned invisible even inside" (Jaleel et al, 2019, para. 22).

(Dis)information blackouts, then, are not information blackouts or Internet shutdowns. They are a combination of the two, where the infrastructural suspension of Internet connectivity is used as a brute force device to create an information blackout where only a few authorized and authoritative information streams are allowed to circulate. It is a critical apparatus that bypasses censorship laws and intermediary liability, and instead uses physical infrastructure disconnection to create filter-bubbles (Pariser, 2011) of curated information that produces singular narratives and squashes almost all resistance and alternative counteractions to reinforce the dominant ideological structure.

Within Internet governance and policy discourses, Internet shutdowns are seen as straightforward questions of access and regulation. The focus is on ways of curbing and controlling information flows and circuits. Civil rights activists and free speech advocates rally against shutdowns, calling out censorship and information blackouts as violations of civil liberties. In these debates, the government authorities fall back on the rhetoric of safety and security, whereas the advocates invoke fundamental rights and the abuse of power. The infrastructure itself is considered value-neutral, and its suspension and reinstatement are seen as the two states of connectivity and disconnection. The state itself propagates the equivalence between Internet shutdowns and information blackouts because it positions Internet shutdowns as a cure to misinformation cycles. For our continued dialogue on the nature of free speech and expression of resistance and protests amid such infrastructural suspension, we are going to have to stop thinking about information resistance only as regulatory disconnection or information censorship. Instead, we will have to start developing a framework where the intentions and implementation of Internet shutdowns are examined more closely through the mechanics, logics, and aesthetics of digital information and computational networks.

In this article, I have argued that the Internet shutdown clearly still makes space for information circulation. The Internet shutdown is more a vehicle by which the state inscribes specific messages with truth-value and silences other dissenting voices. I have presented "(Dis)information blackout" as a condition where we examine the ways in which certain information is produced, stored, circulated, retrieved, and made visible during Internet shutdowns while others become suspiciously latent and often erased from the networks. In decoupling Internet shutdowns from information blackouts, I hope to have offered a different nuance into the rights and responsibilities of activists and protestors, and the need to look at a taxonomy of information as well as the workarounds that emerge from the collective, shared, and community resources of human networks during times of disconnection.

References

Abraham, S. (2019). Intermediary Liability Law needs updating. *Business Standard.* Retrieved from https://www.business-standard.com/article/opinion/intermediary-liability-law-needs-updating-119020900705_1.html

Bashir, S. (2019). The Indian government insists all is well in Kashmir. *TIME.* Retrieved from https://time.com/5659671/kashmir-indian-government/

Brown, S., & Oliver, C. (2019). Q and A: India's foreign minister on Kashmir. *Politico.* Retrieved from https://www.politico.eu/article/q-and-a-india-foreign-minister-subrahmanyam-jaishankar-on-pakistan-kashmir-imran-khan/

Burgess, M. (2018). *To fight fake news on WhatsApp, India is turning off the Internet*. Retrieved from https://www.wired.co.uk/article/whatsapp-web-Internet-shutdown-india-turn-off

Chan, A. S. (2014). *Networking peripheries: Technological futures and the myth of digital universalism.* Cambridge, MA: MIT Press.

Chatterjee, R. (2016, February 9). Student describes what actually happened at the Jawaharlal Nehru University on Feb 9. *Huffington Post.* Retrieved from https://www.huffingtonpost.in/2016/02/15/jnu-arrest_n_9233910.html

Choudhary, M. (2019). *Digital India is offline*. Retrieved from https://thewire.in/rights/digital-india-is-offline

Chun, H. K. W. (2016). *Updating to remain the same: Habitual new media.* Cambridge, MA: MIT Press.

Dijck, J. van, & Poell, T. (2013). Understanding social media logic. *Media and Communication*, *1*(1), 2–14. doi:10.12924/mac2013.01010002

Express News Service. (2015). After Hardik Patel's huge quota rally, wave of violence across Gujarat. *The Indian Express.* Retrieved from https://indianexpress.com/article/india/gujarat/hardik-patel-spearheads-mega-rally-for-obc-quota-demand-in-ahmedabad/

Galloway, A. (2004). *Protocol.* Cambridge, MA: MIT Press.

Ganai, N. (2020). It is a ban on newspapers: Kashmiri journalists on Internet shutdown in valley. *Outlook India.* Retrieved from https://www.outlookindia.com/website/story/india-news-it-is-a-ban-on-newspapers-kashmiri-journalists-on-Internet-shutdown-in-valley/345315

Hafeez, S. (2016). Zee News producer quits: Video we shot had no Pakistan zindabad slogan. *The Indian Express.* Retrieved from https://indianexpress.com/article/india/india-news-india/zee-news-producer-quits-video-we-shot-had-no-pakistan-zindabad-slogan/

The Hindu. (2015). *Gujarat shuts down Internet during exam*. Retrieved from https://www.thehindu.com/todays-paper/tp-miscellaneous/tp-others/gujarat-shuts-down-Internet-during-exam/article8294672.ece

Hoyng, R., & Es, M. (2017). Conspiratorial webs: Media ecology and parallel realities in Turkey. *International Journal of Communication*, *11*, 4219–4238. Retrieved from https://ijoc.org/index.php/ijoc/article/view/6711

HT Correspondent. (2020). No shortage of essential items in J&K, curbs saved lives: Guv Malik. *Hindustan Times.* Retrieved from https://www.hindustantimes.com/india-news/phone-restrictions-helped-save-lives-in-jammu-kashmir-governor-satya-pal-malik/story-YSNWksjorJcx1ss4Ev3M4K.html

Indo-Asian News Service. (2018). Google techie's lynching in Karnataka: How an act of kindness turned deadly. *Business Standard.* Retrieved from https://www.business-standard.com/article/current-affairs/google-techie-s-lynching-in-karnataka-how-an-act-of-kindness-turned-deadly-118071500351_1.html

International Telecommunications Union. (2002). *Constitution of The International Telecommunication Union*. Retrieved from https://www.itu.int/council/pd/constitution.html

Jalan, T. (2020). *"Hooghly district magistrate is at level of additional secretary, can order Internet shutdown," West Bengal govt. in Calcutta HC*. Retrieved from https://www.medianama.com/2020/05/223-west-bengal-govt-hooghly-Internet-shutown/

Jaleel, M., Masood, B., & Akhzer, A. (2019). Kashmir Valley has seen many a lockdown but why this time it is so different. *The Indian Express.* Retrieved from https://indianexpress.com/article/india/valley-has-seen-many-a-lockdown-but-why-this-time-it-is-so-different-article-370-kashmir-amit-shah-5884129/

Kanwal, R. (2016). JNU row: Did a fake video fuel the anti-national fire? *India Today.* Retrieved from https://www.indiatoday.in/india/story/panelists-debate-whether-kanhaiya-sedition-video-doctored-or-not-309451-2016-02-18

Keeling, K. (2014). Queer OS. *Cinema Journal*, *53*(2), 152–158. Austin: University of Texas Press. doi:10.1353/cj.2014.0004

Lakshmanan, R. (2019). *How Hong Kong protestors are embracing "offline" messaging apps to avoid being snooped on*. Retrieved from https://thenextweb.com/socialmedia/2019/09/03/how-hong-kong-protesters-are-embracing-offline-messaging-apps-to-avoid-being-snooped-on/

Langa, M. (2015). Curfew in Gujarat towns after arrest of Patel leader sparks violence. *The Hindu.* Retrieved from https://indianexpress.com/article/india/gujarat/hardik-patel-spearheads-mega-rally-for-obc-quota-demand-in-ahmedabad/

Manzano, M. (1996). *Extensions of first-order logic.* Cambridge, MA: Cambridge University Press.

Mozilla Foundation. (2019). *Internet health report 2019.* Retrieved from https://foundation.mozilla.org/en/Internet-health-report/

Netblocks. (2019). *Evidence of Internet shutdown in Assam and beyond as India pushes through Citizenship Amendment Bill*. Retrieved from https://netblocks.org/reports/evidence-of-assam-Internet-shutdown-as-india-pushes-citizenship-amendment-bill-9AkMJZyD

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy.* New York, NY: Penguin Random House.

Open Net Initiative. (2007). *Pulling the plug: A technical review of the Internet shutdown in Burma.* Retrieved from https://opennet.net/research/bulletins/013

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you.* London, UK: Penguin.

Prasad, R. (2018). Ascendant India, digital India: How net neutrality advocates defeated Facebook's Free Basics. *Media, Culture & Society*, *40*(3), 415–431. doi:10.1177/0163443717736117

Press Trust of India. (2015). Patels vow fresh agitations: Jats to follow. *Ahmedabad Mirror.* Retrieved from https://ahmedabadmirror.indiatimes.com/news/india/Patels-vow-fresh-agitation-Jats-to-follow-suit/articleshow/48747356.cms

Press Trust of India. (2019). What difference does it make? Niti Aayog's VK Saraswat defends shutdown in Jammu and Kashmir. *Financial Express.* Retrieved from https://www.financialexpress.com/india-news/what-difference-does-it-make-niti-aayogs-vk-saraswat-defends-Internet-shutdown-in-jammu-and-kashmir/1828178/

Rajadhyaksha, A. (2011). *The last cultural mile: An inquiry into technology and governance in India.* Bengaluru, India: Centre for Internet & Society.

Reuters. (2018). "He looked like a terrorist": How a drive in Karnataka ended in mob lynching. *Hindustan Times.* Retrieved from https://www.hindustantimes.com/india-news/he-looked-like-a-terrorist-how-a-drive-in-rural-india-ended-in-a-mob-attack-and-a-lynching/story-48MpOGGkqjbDwgv3eigOwJ.html

Roth, K. (2020). *Annual review of human rights around the globe.* Retrieved from https://www.hrw.org/world-report/2020

Schultz, K., & Yasir, S. (2020). India restores some Internet access in Kashmir after long shutdown. *The New York Times.* Retrieved from https://www.nytimes.com/2020/01/26/world/asia/kashmir-Internet-shutdown-india.html

Shaikh, S. (2015). Patel community leader Hardik detained after cops forcibly remove agitators. *Times of India.* Retrieved from https://timesofindia.indiatimes.com/india/Patel-community-leader-Hardik-detained-after-cops-forcibly-remove-agitators/articleshow/48672303.cms

Singh, M. (2019). *India gets more aggressive with Internet shutdowns to curb protests*. Retrieved from https://techcrunch.com/2019/12/19/india-gets-more-aggressive-with-Internet-shutdowns-to-curb-protests/

Sircar, S. & Sachdev, V. (2019). *Why the long Internet shutdown in J&K is doing more harm than good*. Retrieved from https://www.thequint.com/news/india/jammu-and-kashmir-Internet-shutdown-article-370-why-it-is-doing-more-harm-than-good

Software Freedom Law Centre. (2019). *Internet shutdowns.* Retrieved from https://Internetshutdowns.in/

Sundaram, R. (2010). *Pirate modernity: Delhi's media urbanism.* New York, NY: Routledge. doi:10.4324/9780203875421

Thiagarajan, K. (2020). An Indian state tells quarantined folks: "A selfie an hour will keep the police away." *National Public Radio.* Retrieved from https://www.npr.org/sections/goatsandsoda/2020/04/12/828843214/an-indian-state-tells-quarantined-folks-a-selfie-an-hour-will-keep-the-police-aw?t=1586788750972

Watts, D. (2016). *How small is the world, really?* Retrieved from https://medium.com/@duncanjwatts/how-small-is-the-world-really-736fa21808ba