11

Authoritarianism and Populism in the Global South

Limits to Decolonizing the Internet

Caroline Wesson and J. P. Singh

Introduction

Do postcolonial authoritarian states employ decolonization rhetoric to marginalize and surveil groups in their own societies using internet and artificial intelligence? Communication technologies—whether telecommunications, mass media, or the internet—were once posited as increasing pluralism and democratic expectations (Rosenau and Singh, 2002; Norris et al., 2009). The explosion of social media reliant on big datasets and algorithms has now raised concerns about states and big-tech firms being able to control, manipulate, and stovepipe their populations for mobilization and influencing toward radicalized views (Beissinger, 2017; Farrell et al., 2022). While the relationship of the postcolonial state with what was once termed "mass communication"—comprising mostly broadcast and print media—was always problematic in terms of a state's own preferences, mass communication in the postcolonial era, nevertheless, was largely developmental communication meant to foster inclusion and general well-being (Gudykunst and Mody, 2002), The 21st-century variants are more autocratic than developmental. Decolonization means creating a space online where knowledge and perspectives of all are present rather than a space that simply reflects historical and institutional power structures. Exploring the question above illustrates another facet of the limitations of decolonization of the internet, one in which increasingly nationalist and populist leaders in the Global South employ a decolonizing rhetoric to exclude or marginalize various groups in their societies.

Caroline Wesson and J. P. Singh, *Authoritarianism and Populism in the Global South*. In: *Internet Decolonized*. Edited by: Henna Zamurd Butt and M.I. Franklin, Oxford University Press. © Oxford University Press (2026).
DOI: 10.1093/oso/9780197763575.003.0011

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

We arrived at this question from our observations of rising authoritarianism and populist nationalism in the Global South. We note that in these authoritarian countries the internet is often used for surveillance and censorship of the citizenry. This disproportionally impacts marginalized groups within these countries. Another issue here is a lack of proper data protection that allows states to manipulate and punish citizens with their big-data control practices. Ultimately, the internet in these countries operating under authoritarian regimes is another forum for the projection of authoritarian power. We argue that the experience for marginalized groups under colonialism has been mirrored in the postcolonial world with some meaningful differences. Postcolonial states were not adequately prepared to deal with overcoming social stratifications existent in colonial and precolonial societies that persisted into the postcolonial period. These stratifications included practices around race, class, and gender, but in the context of the Global South encompassed others such as ethnicity, religion, and caste. Therefore, state-building projects in the postcolonial societies controlled the historical narrative and current news for developmental purposes (Frau-Meigs and Nicey, 2012). In most postcolonial states, broadcast media were state-owned and often censored, but the articulated ideals were pro-development, inclusive, and secular.

Current authoritarian governments in postcolonial states have co-opted the decolonization and state-building rhetoric to speak against the Global North for excluding them while at the same time disenfranchising media groups within their own countries, most of whom are reliant on the internet for their survival both in terms of solidarity with other groups and for fundraising. Such rhetoric in the developing world features the need for censorship and surveillance for the purpose of securing internet freedoms from outside influence and misuse from colonial powers and Western dominance. The autocratic regimes have also turned to new oppression techniques and tools, to be deployed online and through policies regulating the internet, to manage the "two problems of authoritarian rule." These two problems as articulated by Milan Svolik are the problem of authoritarian power-sharing—or satisfying key groups of elites to sustain rule—and the problem of authoritarian control—which is maintaining control and stability over the governed (Svolik 2012).

The internet complicates matters. It is important for governments to develop capacities for the internet due to its importance for development and economic transformations. But social cleavages and marginalized groups

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

must be managed online—controlling their activities in terms of sharing narratives and organizing. Sympathies toward these groups' narratives must also be managed. It is also important to note that the internet can also be utilized by these authoritarian governments to deliver payoffs to authoritarian elites who support the ruling group/individual—as the satisfaction of elites is important for ultimate regime maintenance.

Under the circumstances outlined above, the internet is not a platform for equality or the incorporation of historically marginalized groups into society. By internet we mean computer networks and communication protocols that increasingly utilize machine learning and algorithms to both generate and recommend information to users. Additionally, internet governance structures, in their current form, heavily predisposed toward engineering protocols and intellectual property issues, cannot hold authoritarian regimes accountable for utilizing the internet as a tool for oppression. These governance structures include the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU), and the World Intellectual Property Organization (WIPO).

The next section provides a brief reprise of the evolution of the postcolonial states and society, and the rise of authoritarianism concurrent with internet technologies. Subsequently, we survey four country cases to illustrate our argument. Decolonization moves at international and domestic levels, entailing questioning of oppressive socioeconomic practice and institutions, remain suspect through internet and AI-enabled authoritarianism.

The Postcolonial State and Decolonization

Postcolonialism in the developing world entailed institution-building and reversing historical trends wherein the (colonial) state had been set up for extractive purposes. While the state is unique anywhere for its monopoly over violence (Tilly, 1985; North, 1990), the colonial state's legitimacy lay not in providing effective governance over those it ruled but for those it represented from the colonial centers of power. The task of postcolonial governance would entail the emergence of a "developmentalist state" that would lend itself materially toward improving the well-being of its citizens and psychologically unshackle the mental traps that colonial oppression had

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

established (Haggard, 2018). The communication instruments of the state were deemed important for a decolonization of the mind (Gudykunst and Mody, 2002).

The developmental agenda of the postcolonial state entailed being at the commanding heights of the societies it governed. The mandate for governance came from the nationalist elites in the developing world that had fought for "independence" from colonial rule. Leaders such as Kwame Nkrumah in Ghana, Jawaharlal Nehru in India, and Suharto in Indonesia epitomized such elite (see Dinika and Redeker, see Oppermann, this volume). Cutting off the exploitative trading ties was important for economic development (Cardoso and Faletto, 1979). Therefore, import substitution industrialization, which encouraged domestic growth over imports, were the norm throughout the developing world. In most of the developing world, heavy manufacturing and extraction industries were state-run. Communication infrastructures—including telecommunications and media—were also state-run and controlled for development messages. In other words, instead of imports, the state led the enterprise of communication and industrialization.

Equally, a decolonization of the mind was necessary. "Where the Mind is Without Fear" a famous poem published in 1910 by India's Nobel laureate poet Rabindranath Tagore, widely available on the internet, articulates such an aspiration. The activism of people such as Frantz Fanon addresses the "dependency complex of the colonized," which produces an internal repression in the mind (Fanon, 2008: ch. 4). Steve Biko in speaking of "black consciousness" or Paulo Freire in Brazil in speaking of "cultural voice" advocated strategies that would liberate the mind of internal repression (Freire, 2018). Similar aspirations are ubiquitous in postcolonial literature. Mariama Ba's *So Long a Letter* or Tsitsi Dungarembga's *Nervous Conditions* articulate the double binds of patriarchy and colonial practices. The tradition of magical realism in Latin America, whether through Gabriel Garcia Márquez or Isabelle Allende, speak to the centuries of colonial history that construct the everyday dominations and conduct among people. In hindsight, the vision of a selfless postcolonial state and decolonizing practices in society unraveled like Greek tragedies killing heroic ideals. The postcolonial state was unable to fulfill its developmental aspirations. Its resource mobilization often resulted in internal rent-seeking or predatory practices that produced corruption rather than development in the heights of power (Singh, 2017). Unable to manage societal demands and stratifications, the communication strategies

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

of the state often articulated unfulfilled promises or populism. Censorship was often at hand to silence voices.

The historical roots of the postcolonial state and decolonization endeavors, such as self-governance, strengthening of identity, and empowerment, are necessary for understanding the current trajectory of authoritarianism articulated through the internet in many developing countries. The roots of this authoritarianism lie in problems of governance over heterogeneous societies in the developing world that varied from caste groups in India to ethnic tribes in Kenya. Understanding this history is not an excuse for overlooking authoritarianism, but a reason for analyzing the sharp-edged instruments the postcolonial state developed for controlling and censoring societal dissent (see, for example, Bates, 2005 on Kenya; Rudolph and Rudolph, 1978 on India). The current authoritarian state in the developing world often, in fact, deploys a populist "decolonization" narrative to defend its practices.

Scholars have argued that the internet is a powerful tool for repression in the hands of autocrats in relatively young democracies (Rød and Weidmann, 2015; Sinpeng, 2020). In many cases, online discourse and organization can be more easily surveilled and controlled than non-online actions, granting governments new opportunities for monitoring civil society and potential opposition groups (Howard, 2010; Kyriakopoulou, 2011). This is especially true as technologies for surveillance have become more readily available, especially as China has sought to increase exports of these technologies both in bilateral arrangements and through their Digital Silk Road program (Ververis et al., 2020; Greitens, 2020). Some countries have sought these technologies as solutions to valid concerns about crime, while some may also deploy these technologies for the purpose of managing opposition groups (Greitens, 2020). Research has shown that autocracies and weak democracies are more likely to import surveillance AI systems from China, especially in years of domestic unrest (Beraja et al., 2023).

Two dominant strategies of the authoritarian state help to understand the limits of decolonization: data sovereignty and surveillance. China and India have led the way with "data sovereignty" claims, meaning that data about their citizens must be collected and maintained within their sovereign borders. The link to early postcolonial self-sufficient economic strategies can be easily made, and the fears that data about citizens on the internet can be easily exploited internationally is equally well-founded. In reality, such data have empowered authoritarian states with capabilities to monitor citizen activities. These include social score cards and linking almost

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

every internet transaction to digital identity cards in China. Issues around the Chinese model of data sovereignty have also been raised around Chinese internet communications technologies, as some have found that when countries accept technologies from Chinese companies, they must comply with Chinese data policies and surrender domestic user data to the Chinese government (Gravett, 2020; Wright, 2021).

The second strategy is censorship and surveillance. The deployment of surveillance technologies, restrictions on civil society dissent, and restrictions in press freedoms have proliferated the world over. The postcolonial states were concerned with information flows that always cast them in a negative light (Frau-Meigs and Nicey, 2012). The developing world was perhaps rightly concerned that information flows were from the North to the South and that most "news" about the South was negative and stereotypical (poverty, famines, violence, and corruption). The advocacy for a New World Information Communication Order in the 1970s and the World Summit for Information Society in the 2000s sought to correct the flows and imageries (Singh, 2012; see Franklin, this volume). With the rise of authoritarian governments, information flows have taken on the added dimension of domestic censorship and surveillance in societies that were broadly pluralistic earlier. In some cases, civil society learned behaviors of self-censorship when faced with ambiguous and asymmetric regulation of language and behaviors online (Druzin and Gordon, 2018).

Cases

To examine if postcolonial states employ decolonization rhetoric to marginalize and surveil groups in their own societies, we have selected four country cases. These case studies are structured to present the rhetoric of the government at a given time and how decolonization rhetoric is employed to marginalize, surveil, and/or censor groups that exist within the country's society. For this chapter we have selected four cases: Brazil under Jair Bolsonaro, Mexico under Andrés Obrador, Indonesia under Joko Widodo, and India before and during the Narendra Modi government. The cases include populism from the left (Obrador in Mexico, Widodo in Indonesia) and from the right (Bolsonaro in Brazil, Modi in India). They also include countries with viable opposition in legislature (Brazil, Mexico) versus the lack of it (India). Populist and authoritarian leaders seek to destroy or silence all

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

opposition within the government and civil society, and our cases described below detail these measures.

Current forms of populism in the Global South derive their legitimacy from various types of nationalism and recall colonial tropes for who is to be included in the "national" projects they envision. Leaders such as Modi and Obrador built their careers in speaking to their local roots that allow them to speak against the "West." Widodo has sought Chinese investment with the claim to end Western exploitation of its resources. When the United States and Germany critiqued arrests of opposition leaders before the 2024 elections in India, the Vice President of India, Jagdeep Dhankar, was quoted as follows: "We are not a nation to get scriptures from others. We are a nation with a civilizational ethos of more than 5000 years" (Shih, 2024). Meanwhile Prime Minister Modi and political leaders from the Bharatiya Janata Party (BJP) frequently referred to the 200 million Muslims in India as infiltrators during the 2024 parliamentary elections.

Brazil

Issues surrounding internet surveillance and censorship began in earnest in Brazil following the start of the Jair Bolsonaro presidency in 2019. The rhetoric and use of internet to control and censor political dissidents under Bolsonaro are characterized by Bolsonaro and allies' use of both disinformation campaigns and regulatory policies seeking to force social media platforms to comply with the President's idea of "permissible" content online. Disinformation campaigns lodged by Bolsonaro and his supporters have largely gone unchecked, and continued post-presidency, even influencing major physical demonstrations in 2023. There were some "checks" on the Bolsonaro administration's attempts to force social media platforms to comply with their ideals for content moderation from the Supreme Court and Senate, but the targeted disinformation campaigns have reduced trust in electoral systems, and some policies have limited accountability for the speech of elected officials online. These disinformation campaigns sought to reduce trust through approaches that illustrated government institutions as incompetent (particularly illustrating this through the handling of the COVID-19 pandemic) and the election as illegitimate by making claims about electronic voting systems and the more general voting process (Muggah, 2022). Much of this work was said to be carried out by an "Office of

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

Hatred" or cabinet staffed of individuals coordinating the misinformation and attack campaigns on the opposition to the administration (Ozawa et al., 2023).

One of President Bolsonaro's first moves toward greater internet surveillance was the creation of the Citizen's Register, a database that would consolidate citizen data held by government institutions into one database (Kemeny, August 19, 2020). Outside watchdog groups have noted that there are major concerns about abuse of the system, as it was created without any public consultations or consent. Citizen's biometric data has also been compiled into the database, including images and retinal scans, which may be used with facial recognition applications. There are also concerns about the overall security of the system, as it has resulted in the centralizing of a large amount of individual data. Concerns over the database's creation have been exacerbated as Brazil has sought to, and has, acquired Chinese surveillance technologies (Canineu, May 31, 2019).

Bolsonaro's rhetoric surrounding the 2022 election, which he ultimately lost, sowed distrust in the election technology and administration. It targeted those within the government and civil society who opposed the Bolsonaro administration, employing tactics that had been used in other countries including Russia and the United States. Primarily, these tactics were those in which individuals and bots on Whatsapp, Facebook, Twitter, and other platforms worked to target opposition groups (with emphasis on the Worker's Party), news outlets, and journalists publishing stories unfavorable to Bolsonaro (Ozawa et al., 2023). The use of the platform Whatsapp has been noted as particularly important, as, due to the application's end-to-end encryption technology, it is more difficult to identify disinformation campaigns when compared to other platforms such as Facebook and Twitter (now known as X) (Nemer, 2021). In 2020 the administration passed a "fake news" bill, which has been consequential, as it places limits on holding elected officials accountable for speech online, thus giving a "free pass" for officials to make statements that may undermine public institutions, including elections, and smear opposition groups (Santos, April 24, 2023). Another attempt to support the disinformation campaign was an effort to regulate U.S.-owned social media companies' content moderation policies, as the administration claimed that such companies arbitrarily removed content from their platforms specifically related to COVID-19 and then then upcoming 2022 election. These efforts to force the hands of social media platforms to keep content deemed to violate their terms and services ultimately failed

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

due to intervention from the Supreme Court. Additionally, as of 2023 Brazil's electoral court has banned Bolsonaro from office until 2030 for his false claims regarding the election (Kahn, June 30, 2023).

It would be in the state's interest to act counter to this and preserve the freedom for online discourse. Yet there is a delicate balance, given that typically the head of these campaigns is the head of state, which would place the burden to act upon other government institutions. The issue stands though that under Bolsonaro this rhetoric was being co-opted and used to root out dissidents and opposition groups. Ultimately though the Brazilian court system did not find the argument that social media platforms were arbitrarily removing content compelling and blocked some measures the administration attempted to pass from going into effect. After the election of President Luiz Inácio Lula da Silva (Lula) there were developments to change the way disinformation is addressed in Brazil. President Lula created two new departments, a working group, and other online resources to assist with reporting responding to disinformation (Hernandez-Roy and McKenna, 2023). Much of this approach is seeking to hold social media companies responsible rather than candidates disseminating disinformation; the same can be said for the Fake News bill, which has reemerged as a potential solution to the continued persistence of disinformation's challenge to democratic institutions (Hernandez-Roy and McKenna, 2023). The focus has shifted toward the responsibility of the ever-present Western social media giants and their reach into society to host information that is critical in shaping public opinion.

The emphasis on Western social media giants culminated with the August 2024 banning of Elon Musk's X (formerly Twitter). Supreme Court Justice Alexandre de Moraes had ordered X to appoint a new legal representative in Brazil after the social media company's legal representative had refused to comply with requests from Justice Moraes to ban specific accounts he accused of spreading disinformation (da Silva and Buschschlüter, September 2, 2024). These accounts were primarily supporters of former President Bolsonaro, and representatives from X claimed that the demands to block these accounts were akin to censorship and refused to do so (da Silva and Buschschlüter, September 2, 2024). Therefore, Justice Moraes had X banned in Brazil. As of late September 2024 the social media website remains banned, but Musk had walked back his previous statements that X would not comply with demands from the Brazilian government and agreed to pay a fine to the government and comply with government demands for content

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

moderation on the platform (Brito and Magalhaes, September 26, 2024). The final conclusion of this dispute has yet to be seen at time of writing. This development and the involvement of the Supreme Court in these matters seem to suggest a continuance of government intervention in matters of internet governance for political ends.

Indonesia

The Indonesian government under President Joko Widodo has taken an active position in surveilling and censoring the internet for the purpose, they argue, of protecting the citizenry from negative and harmful content that disturb the peace of society. Therefore, the government acknowledges a mandate to take care and protect citizens but has determined that they are also to make decisions about what might harm society. The government has mainly targeted information related to minority groups including the LGBT+ community, communities critical of Islam, and groups critical of the Indonesian government or those who might advocate for independence of the Papua region (Freedom House, 2022a). The Widodo government has passed new legislation that outlines what information and groups are to be censored or blocked and new regulations requiring social media platforms, search engines, online companies, and mobile applications to register with the government for the purpose of overturning user data requests and complying with content laws. While the government has couched these interventions in online life in terms of safety, they have targeted minority groups that threaten either the sitting government or the status quo of Indonesia.

A flurry of new legislation and action in this area began around the same time as the start of the COVID-19 pandemic. In 2020 Ministerial Regulation Number 5 (henceforth MR5) was passed. This controversial law empowered the government to perform censorship and internet regulation through a few new channels including registration programs for companies, blocking websites, and bringing forward new guidelines for content to be targeted for removal (Freedom House, 2022a). Under MR5 companies had to comply with registration through the Ministry of Communication and Information Technology or they would be blocked. The purpose of registration was to designate a contact in Indonesia who could correspond with the government if there were issues with content regulation

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

compliance. In some instances, companies have faced large fines for content that does not meet Indonesian standards. Additionally, MR5 requires registered companies to turn over user data—which can be requested without a court order (Human Rights Watch, 2021a). This provision has caught the attention of many human rights and data privacy watchers, as it can allow the government to quickly access user data of those it may deem unfriendly (Human Rights Watch, 2021a). Several international websites were blocked under MR5 in 2022 for not meeting the registration deadlines. MR5 has concentrated surveillance and censorship of the internet in the government's hands, and the policy was never put up for public comment, therefore becoming law without any civil society consultations. Not long after the passage of MR5, new police units were formed in 2021 to increase monitoring of social media posts and ensure that such posts were in line with the Indonesian Information and Electronic Transaction Act. These police units claim to focus on hoaxes and misinformation but have also been utilized to monitor content that the government believes could materialize into "public disorder." Some observers believe the creation of these units was in response to protests of a job creation law in 2021 (iTnews Asia Team, 2023).

Another major issue for internet access, censorship, and surveillance is several reported internet outages in the Papua region that have coincided with events in the region related to the Papuan independence movement (Freedom House, 2022). There has also been significant censorship of news of human rights violations in Papua, and in many cases news sites related to the region have been completely blocked for viewing. This issue is currently ongoing as well. Therefore, internet censorship has taken a role in this instance to silence a minority group rather than simply remove harmful content. Finally, evidence from Citizen Lab in 2015 supported that the Indonesian government had deployed FinFisher spyware, potentially with the goal of cracking down on journalists and activists who might be involved in reporting stories that may result in unrest (Bill Marczak et al., 2015). This entailed government deployment of the FinFisher spyware products (a commercially available surveillance malware software) to collect data and information on individuals of interest, which may have been those posing terrorist threats, but there are allegations of use of the spyware to target West Papuan Independence activists, journalists, LGBTQ+ activists, and members of religious minorities within Indonesia (Rappler, 2016). The Citizen Lab report does detail that some usage of this technology may be out of

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

concerns about terrorist attacks but also might be related to independence movements in Papua and Central Sulawesi (Bill Marczak et al., 2015). Freedom House has also connected the monitoring of online activity to offline physical violence toward journalists as well, including a journalist who was a victim of a stabbing he claims was likely connected to his reporting, acts of vandalism on the property of journalists, and bombings. These incidents have been documented in more detail by Freedom House (2022).

There have been additional developments in internet surveillance and data privacy in Indonesia. For instance, as of November 2023 the government passed a new policy that requires digital IDs for citizens (Digital Watch, 2023). The ultimate impact of this policy will need to be evaluated in the future, but the government has advocated efficiency as a reason for its introduction. It can be seen that in the last few years there has been a change in how the Indonesian government is approaching internet governance issues, specifically those that are related to content moderation on social media, content-sharing platforms, streaming services, and communication platforms, with the introduction of MR5 (Human Rights Watch, 2021a). MR5's focus is to ensure that companies comply with laws surrounding permissible content, but critics of the legislation state that it is a tool for censorship and surveillance (Human Rights Watch, 2021a). While there might be honest reasons for censoring and monitoring some activity online, there are several instances in which minority groups have been targeted with little to no justification. Particularly the incidents in the Papua region are concerning, as they involve not just censorship and surveillance, but also moments of service denial altogether, eliminating a mode of communication for individuals in the region.

Mexico

Issues around internet governance, surveillance, and censorship began to capture headlines in Mexico in 2020. During this time President Andrés Obrador began to use rhetoric that oversight and watchdog groups needed to be eliminated, stating that they were useless organizations and that the government would naturally do what it needed to protect the people, without the involvement of these institutions. His government recognized the imperative for protecting individuals while online but moved to remove several safeguards put in place by previous administrations, passing legislation

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

that would change how much social media platforms could participate in content moderation, and engaged in well-documented disinformation campaigns. Obrador's administration sought to control who and in what cases speech should be protected online.

There has been a detailed history of attempts to remove undesirable political content from the internet in Mexico. The state has openly threatened legal action over posts made by journalists, and watchdog groups have reported several instances of aggression against journalists reporting on sensitive matters in the country since 2021 (Freedom House, 2022). Citizen Lab has reported that Pegasus spyware software has been deployed on journalists operating in Mexico (Scott-Railton et al., 2022). Interestingly, Obrador noted a spying problem in the country, but claimed that under his administration spying on opposition groups and journalists had stopped, despite Citizen Lab reports finding instances of spyware use since Obrador's election (Reuters, 2022).

Importantly, Obrador also spoke out against social media companies banning users from posting on their platforms—arguing that companies should not be allowed to limit individual's freedom of speech (Reuters, 2021). He articulated this stance on multiple occasions, including in international forums where he advocated for President Donald Trump to be re-platformed following his ban on several social media platforms (Weiss, February 10, 2021.). Obrador's political party moved to pass legislation that would take content moderation from social media platforms and move it into the hands of the Federal Telecommunications Institute—giving the government the final say in how and when to delete content and block users from platforms (Human Rights Watch, 2021b). At time of writing, this bill had not passed through the Senate, but it does articulate the administration's aspiration to gain control over content moderation. This is likely linked to Obrador's frequent discussion of the pervasive "fake news" surrounding a variety of Mexican political issues and previous election cycles, including the 2018 election (Armstrong, August 2, 2018). It is important to note that Obrador and his allies have also been accused of spreading disinformation (Vivanco, 2020).

New developments in this space are occurring rapidly. As of December 2023, a new proposal was made by President Obrador to eliminate Mexico's national transparency agency, the Instituto Nacional de Transparencia (INAI) (Associated Press, 2023). The President characterized the agency

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

as being too expensive to maintain and ultimately "useless," as the government already performs activities that keep the internet safe (Mexico News Daily, 2021). This reflected an attitude of hoping to bring matters of internet governance, surveillance, and censorship under the direct control of the President's administration rather than housing it within an independent institution. The sentiment reflected the President's desire for control over the internet and ongoing campaigns to monitor and control opposition groups.

In June 2024 Claudia Sheinbaum was elected to be the next President of Mexico. It has yet to be seen if there will be major changes in approaches to internet governance, but it is important to note that Sheinbaum was endorsed by Obrador. During her campaign for election Sheinbaum emphasized the need for a "complete digital transformation" in Mexico and proposed plans for improving internet access and government service provision through the internet (Valverde, June 4, 2024). While the Obrador administration and the Sheinbaum administration have vowed to change course from previous administrations' usage of spyware and opposition targeting, not much has appeared to change. The Sheinbaum government has remarked that it has effectively taken care of all matters of internet governance and protections for users online, but it does so as it seeks to eliminate independent transparency agencies that have been created by previous administrations to tackle these issues. Additionally, the number of journalists experiencing targeting via spyware demonstrates continued efforts to crack down on unfriendly information and opposition groups.

India

Internet repression has grown in India since 2014 after the Narendra Modi government came to power, but the antecedents can be traced to an interfering postcolonial state with a meritocratic bureaucracy that wield enormous power. State control over society through the internet has taken two forms: first through the issuance of a national digital ID, and second through an increasing crackdown on civil society and media, including the use of information campaigns to repress dissenting views. Social media companies are also ordered to follow state commands, especially Twitter/X and Facebook, which were asked to turn over user data including metadata and searches.

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

India has a digital ID for citizens named "Aadhar" that began to be rolled out in 2009. In 2023 it covered 95% of India's 1.4 billion population. While initially opposed to the Aadhar project, Prime Minister Modi had a turnaround after coming to power in 2014. The provision of a digital ID, and later bank accounts linked to this ID, were important for the provision of state services including welfare payments from the state from hundreds to millions of people, run through the Unique Identification Authority of India, which is an entity under the Ministry of Electronics and Information Technology. Aadhar has become the de facto ID for proving one's identity in India and to access everyday services such as banking and communications. The digital ID is undoubtedly a major innovation from India and now being emulated in many parts of the developing world (Nilekani and Shah 2016). Nevertheless, without adequate data protection laws and leakages of individual data, the civil society group Internet Freedom Foundation successfully challenged the Aadhar platform at the Supreme Court in India, leading to a historic judgment declaring a fundamental right to privacy in India in 2017. Successive attempts to pass a data protection bill in India were unsuccessful until the 2023 Digital Personal Data Protection Act, which provides broad leeway to the state to monitor citizen data (Mathi, November 19, 2022).

The Aadhar platform and the financial infrastructure that rests upon it have revolutionized digital payments and delivery of public goods in India. The identity and the financial layers are called "India Stack" ("India Stack," 2023). But the material provision of digital services is different from the privacy and civil rights concerns that have emerged alongside it. The Modi government has spoken about "data sovereignty" issues in maintaining strict controls over data storage and flows, which has especially disadvantaged international firms operating in India, including social media platforms. The government has not been shy about deploying an explicitly postcolonial rhetoric about India as an emerging power, while at the same time justifying data controls as a necessity for such emergence.

The crackdowns and control over news and social media have especially increased in the last five years (Mehrotra and Menn, November 8, 2023). In 2022, Twitter even sued the Indian government for being asked to remove content repeatedly. The Modi government has been associated with a far-right "Hindutva" agenda that has often resulted in violence against minorities, especially Muslims and Christians. Forms of dissent in news media are almost negligible now. Most news media outlets are owned by

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

Modi supporters, and independent journalists have received threats and beatings. The government rarely condemns these practices. In 2023, India ranked 161 out of 180 countries in the World Press Freedom Index. It ranked at 80 in 2002. The government has been especially active in the propaganda and surveillance space. In 2021, journalists reported the widespread purchase and use of Pegasus spyware by the Indian government to spy on the opposition, critics, and the press (The Wire,'" March 31, 2023). Reported attacks using the Pegasus system occurred in late 2023 ("India targeted high-profile journalists with Pegasus spyware: Amnesty," 2023). Additionally, as early as 2019, there has been evidence of the Indian government deploying the Pegasus system to crack down on civil rights activists, including those calling for the release of other prominent civil rights activists, particularly the Bhima Koregaon 11 (Aljazeera 2023; Amnesty International, 2020). As with other authoritarian leaders, the Modi government has increased the use of disinformation and propagandist claims. The co-option of the postcolonial rhetoric is especially evident in the way that social media aligned with, or originating from, the Modi government counters any claims of declining press freedoms or forms of violence against minorities as emblematic of a colonial mindset that dismisses India's achievements (Shih et al., December 19, 2023). Critical stories are dismissed as "western propaganda" aligned with powerful capitalist interests. George Soros is often cited as funding such claims in the West (Agarwal and Pal, 2023). Nevertheless, the mid-2024 general elections reduced the parliamentary majority for Modi-led BJP parties and allies. It remains to be seen if internet freedoms will be restored and citizen surveillance decreased.

Conclusion

In many cases, postcolonial states around the world were gazed upon with optimism as they transitioned into independence (see Dinika and Redeker, this volume). Many mid-20th-century leaders held the hope of the citizenry for a brighter future featuring both economic development and robust representative institutions. This mandate for both development and a more inclusive form of governance should have empowered leaders to fulfill their social contract with citizens, but history shows a mixed record. In some postcolonial states, existing or new social stratifications were never managed in a way that brought these groups into society. Marginalization of minority

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

groups continued as a way to manage any opposition to the new regime's rule. There are plenty of examples of these social cleavages being managed by regimes through policing, resource extraction, political or economic exclusion, and other tactics. The advent of the internet has provided both new challenges and opportunities for new authoritarian postcolonial regimes to surveil and censor opposition groups they perceive as a challenge to maintaining the status quo, or as obstacles to their further retrenchment. The unprecedented amount of access to details about individuals' personal information, thoughts and ideas, and movements, all in an accessible record, has never existed before, enabling a level of surveillance and censorship on a new level globally. New authoritarian governments must determine how to manage long-standing social cleavages. Proper management of these cleavages would mean these governments include marginalized groups and go through processes of reconciliation and social transformation. Yet, it is likely that in order for these authoritarian regimes to satisfy the desires of social elites, or pockets of society with more power politically, socially, or economically to secure and stabilize rule, there will be further marginalization or surveillance of excluded groups. The internet, with a particular emphasis on social media due to its two-way communication potential through which people can engage with one another, introduced a new environment for organizing and sharing perspectives—including political criticism and mobilization of opposition groups. This chapter explored the way in which postcolonial authoritarian regimes are seizing a variety of internet tools to manage marginalized and opposition groups online, which has tangible impacts on how these groups operate offline, through four illustrative cases: Brazil, Indonesia, Mexico, and India.

Each of these cases features a leader (outgoing or reelected) who leans into decolonization rhetoric to empower their administration to utilize a variety of tools to manage opposition groups and marginalized societal groups online. In each case, a bureaucracy, often selected through highly meritocratic processes, has implemented these policies. Dissent among competent bureaucrats is not rare but often silenced through dismissals, transfers, and even violence. Typically the model follows that the leader introduces some warning about online discourse, maybe centered on concerns about public safety, overreach of large Western social media companies into public discourse regulation, or the spread of "fake news." Leaders empower themselves to act in a manner they argue is reasonable to protect the public from these threats, but the reality is a manipulation of this situation, in which the leader

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

seizes the opportunity to surveil and censor groups and individuals it deems hostile.

In the case of Brazil, Bolsonaro sought to introduce new policies that would place content moderation in the hands of the Brazilian government rather than large Western-dominated social media companies, which he claimed were biased and arbitrarily removing content. Bolsonaro directly tied these behaviors to a call for the government to protect the people's freedom of speech, while the reality was to safeguard his content from removal on platforms as he spread disinformation regarding electoral processes in Brazil. While the regime's desired policies were mostly struck down, provisions protecting elected officials' speech have been maintained. In Indonesia, much of the rhetoric utilized by the government has couched internet surveillance and censorship in concerns about public and social safety. The government under Widodo has empowered itself to remove content that does not fit with desired cultural values, and to limit or completely halt, discourse and reporting on sensitive issues such as Papua's movement for independence. The government's consistent emphasis on the need to protect the populace has been wielded against multiple groups that might bring forward new social movements that the current regime has avoided managing. In Mexico, Obrador's presidency was particularly aggressive in efforts to limit journalists and activists from reporting on matters that might paint the administration in an unfavorable light. The regime argued that it had taken full and appropriate responsibility for matters of internet governance and had sought to protect individual freedoms online; for example, when social media companies "overstepped" in unfairly banning individuals from their platforms or failing to properly deal with fake news. These calls for protection of freedoms and concerns over "fake news" led to the government proposing reforms on content moderation: Yet another example of leadership employing the language of protection for the purpose of consolidating control over the internet governance apparatus. Meanwhile in India, the Aadhar system has been one that the Modi administration has touted as good for economic development and efficiency in public goods provision. Yet, the system has resulted in the consolidation of massive amounts of citizen data at a moment when the administration has been increasingly cracking down on opposition groups and their discourse. While the government is articulating efforts toward more efficiency and streamlined transaction processes, citizens are left vulnerable, especially those who identify and engage with the opposition.

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026

The rhetoric in these cases has a common through line. Each government speaks to a need to protect the public or provide an internet service that would assist in reaching goals of economic or governmental efficiency. These rhetorical ambitions, to protect and to serve, have then been co-opted by authoritarian governments with their own preferences to stay in power despite opposition groups both off- and online. The tools presented by the internet to manage these groups are just as powerful as the internet's potential to act as a forum for community organizing. These governments are eager to seize these tools while operating under the veneer of a responsible custodian of the internet.

Downloaded from academic.oup.com/book/63443/chapter/577422349 by University of Delaware user on 05 November 2026