Democracies Can Become Digital Dictators

Justin Sherman

Internet shutdowns are an increasingly popular tool for digital repression. It's what many in wealthy, liberal democratic countries can't ever imagine happening—authorities blocking access to social media or services like WhatsApp, or even cutting internet access altogether, in the wake of mass assemblies, protests, or unrest.

These shutdowns have happened in Egypt, Zimbabwe, Iraq, and many other nondemocratic countries. Studying these incidents, a pattern starts to emerge: Citizens take to the streets; the government chooses to resist the resistance; and they shut down the internet under the guise of halting unrest. Underlying this pattern are weak or nonexistent checks and balances on government power that enable authorities to black out communications in the first place.

WIRED OPINION

ABOUT

Justin Sherman (@jshermcyber) is a cybersecurity policy fellow at New America.

Yet India—the most populous democracy on earth—recently shut down the internet in the state of Assam (population: 31 million) after citizens protested a highly controversial citizenship law passed at the end of 2019. Services were then cut in Meghalaya, Tripura, West Bengal, Uttar Pradesh, and elsewhere. This comes after India led the world in web shutdowns in both 2018 and 2019. India's case highlights how internet repression isn't confined to dictatorships.

Contrary to long-standing narratives about the "borderlessness" of cyberspace, the internet can absolutely be controlled by the state. Talk of "cyberspace" and the "digital domain" might invoke images of some imaginary space up in the air (or the cloud), but the internet is still composed of undersea cables, server farms, endpoint devices—all physical things. The internet isn't always easy to control. Governments might need to build or purchase sophisticated technical capabilities to do so. But it's certainly possible.

To this end, various regional governments in India have exerted control over parts of the internet in their borders to execute internet shutdowns. Riots and misinformation have been driving forces here, with problematic interplays between the two—a rash of cases where misinformation went viral on WhatsApp in India and subsequently led to violence. A September 2019 court decision, for instance, ruled that national security concerns could permit Indian authorities to shut down the internet despite concerns about free information access.

As WIRED has reported, the Indian government has asked WhatsApp for the ability to track and stop certain messages, conveniently "failing to sufficiently address underlying issues of intolerance, weak policing, caste divides, and nationalist rhetoric that has fueled violence again and again." WhatsApp has denied these requests, so various governmental entities have turned to internet shutdowns as a result.

That said, it's unclear if network shutdowns actually work to halt the spread of misinformation—further study is needed on the issue. Absent desired capabilities to monitor the internet within their borders, governments may want to at least do *something* (i.e., shut down web services) in light of misinformation-fueled riots; there could be legitimate motivations in certain cases.

But this doesn't mean internet shutdowns aren't repressive. To kill communications systems upon which citizens, businesses, emergency personnel, and others depend is an affront on the global and open internet and likely exacerbates ongoing violence. Even if protesters can still communicate and organize by word-of-mouth, shutdowns (in the eyes of authorities) may serve to at least disrupt mass organization and prevent outsiders from looking in.

India's ongoing communications blackouts are a prime example of this blunt form of digital repression applied with highly questionable motivations. And despite a high court ruling about a week later that the Assam government must restore communications in that part of India, officials appear to have ignored the decision. The deferral of this issue to the courts may create additional problems given the presently high costs of network shutdowns and the long review process of the judicial system.

All of this underscores how it's not impossible for internet shutdowns, and digital authoritarianism in general, to arise in democracies, particularly when justifications revolve around public safety. India's case shows that network shutdowns don't have to be nationwide, as they have been in many authoritarian countries (the recent Iraq shutdowns were near-total). In theory, with the right layout of physical internet infrastructure, they could be concentrated in certain geographic areas.

Weak checks and balances on government internet control may also enable internet blackouts in countries that are largely or otherwise not authoritarian. It's the same underlying problem with problematic surveillance practices that have cropped up in democracies, where the right laws and regulations have not yet been implemented or enforced.

India's case also highlights legitimate democratic fears about misinformation, as well as how misinformation can be top cover for internet repression. Smaller countries with less evolved internet policies could, in this vein, find internet blackouts to be appealing should they lose sleep over thoughts of viral fake news and the incitement of violence. Chinese state media have already capitalized on recent events to say that it's a "routine operation for governments all over the world to manage the internet based on national interests, including shutting down the internet in a state of emergency," citing the government's previous shutdown in Xinjiang.

This matters for human rights and free speech. It also matters because of the violence that often revolves around, or is perhaps even fueled by, web shutdowns. But it also has a deeper, geopolitical dimension. Democratic countries are increasingly questioning how an ideal democratic regulation of the web looks in light of growing harms like cyberattacks and nation-state-coordinated disinformation campaigns, a la Russia in the 2016 US election. The last decade's events have shown that total internet openness comes with security risks.

Certain things about India's case are unique. As I have previously written, the Indian government has advanced a series of mixed digital policies that could be considered democratic in some ways and authoritarian in some others. Even the Personal Data Protection Bill recently introduced into parliament has pro-privacy clauses alongside potential loopholes for government surveillance. Also, the Modi government's crackdowns on Kashmir—another site of frequent web shutdowns, and now the longest such blackout in a democracy—capture some of the particular ethnic and religious tensions that plague the country, and the current leader's work to reshape national identity.

But as a democracy with nearly 1.4 billion people, and with a rapidly growing digital economy, India's actions in the cyber sphere have pronounced impacts around the world. Nations with less-developed or less-regulated internets will look to India, the US, Japan, the UK, Australia, and other democratic powers for guidance on internet governance. As we rightfully continue to call out and combat digital authoritarianism and internet shutdowns in dictatorships, we should remember to also do so when democracies engage in the same repressive behaviors.

WIRED Opinion *publishes articles by outside contributors representing a wide range of viewpoints. Read more opinions here. Submit an op-ed at opinion@wired.com.*

Justin Sherman (@jshermcyber) is a Cybersecurity Policy Fellow at New America.