



TARGETED, CUT OFF, AND LEFT IN THE DARK

The #KeepItOn report on internet shutdowns in 2019

#KeepItOn 

A note on our data

This #KeepItOn report looks at incidents of internet shutdowns in 2019. While we try to be comprehensive, our data relies on technical measurement as well as contextual information, such as news reports or personal accounts. The constraints of our methodology mean that there may be cases of internet shutdowns that have gone unnoticed or unreported, and numbers are likely to change if and when new information becomes available.

#KeepItOn

The #KeepItOn campaign unites and organizes the global effort to end internet shutdowns. The coalition is growing rapidly, and so far 210 organizations from 75 countries around the world — ranging from research centers to rights and advocacy groups, detection networks, foundations, and media organizations — have joined the movement.

This report is a publication of Access Now for the #KeepItOn coalition and was written by Berhan Taye with the collaboration of Access Now's team.

The author would like to specially thank Melody Patry, Sage Cheng, Peter Micek, Donna Wentworth, Carolyn Tackett, Gustaf Björkstén, Akash Singh, Raman Jit Singh Chima, Verónica Arroyo, Laura O'Brien, Emna Sayadi, Billie Goodman, Madeline Libbey, and Jennifer Brody for their contributions. We would like to thank Marianne Díaz from Derechos Digitales, Andrés Azpúrua from VeSinFiltro, Peace Track Initiative, Software Freedom Law Center, India (SFLC.in), Southeast Asia Freedom of Expression Network (SAFEnet), Media Matters for Democracy, and other members of the #KeepItOn coalition for contributing and reviewing data and providing valuable information about cases.

Table of contents

I. Internet shutdowns in 2019: a global overview	1
Internet shutdowns in Africa	3
Internet shutdowns in Asia	3
Internet shutdowns in Latin America	3
Internet shutdowns in Europe	3
Internet shutdowns in the Middle East	3
II. New trends observed in 2019	4
Longer shutdowns	4
More targeted geographical scope	5
Shutdowns are affecting more people in Africa	6
Venezuela's online crisis: internet shutdowns	7
III. Networks, services, and communications affected by internet shutdowns	9
Services affected in 2019	9
If you can't shut them off, slow them down!	10
Social media blocking	10
IV. What do the governments say?	12
Do governments ever acknowledge internet shutdowns?	12
How did governments justify shutdowns in 2019?	13
V. Elections, protests, and shutdowns: What we know from 2019	14
Elections and shutdowns	14
Protests and internet shutdowns	15
VI. Judges raise the gavel to #KeepItOn around the world	17
VII. Business as usual — India tops the list of countries ordering the most shutdowns in 2019	19
Kashmir: the world's second-longest shutdown in 2019	20
VIII. Rohingya disconnected at home and abroad	21
Myanmar: disconnected at home	21
Bangladesh: disconnected abroad	21
IX. The #KeepItOn coalition in 2019 and 2020	22
Engaging with governments and international bodies	22
Grassroots grants help #KeepItOn	23
Challenges and opportunities	23

I. Internet shutdowns in 2019:

A global overview

From Bolivia to Malawi, India, Sudan, and beyond, 2019 was a difficult year, online and off. The #KeptOn coalition has documented an increase in internet shutdowns¹ in 2019, as well as a trend toward sustained and prolonged shutdowns, and targeted internet shutdowns.

213 Documented shutdowns in 2019

We added new and repeat offenders to the internet shutdown shame list. While at least 25 countries shut down the internet in 2018, members of the #KeptOn campaign and Access Now have documented shutdowns in more than 33 countries in 2019.

Number of countries that shut down the internet

33
in 2019

25
in 2018

Democratic countries, those under authoritarian regimes, and countries in transition have all disrupted internet connections for months at a time. Benin, Zimbabwe, Eritrea, Gabon, and Liberia are some of the countries new to the list in 2019.

In 2019 we documented at least 213 incidents of internet shutdowns around the world. Just like in 2018, India tops the list globally of countries that have shut down the internet, with a staggering 121 incidents of shutdowns, including in new states that shut down the internet in an evident attempt to stifle dissenting voices.² Following India, Venezuela was a global “leader” for shutdowns, blocking access to social media platforms at least 12 times in 2019. After Venezuela, Yemen, Iraq, Algeria, and Ethiopia were the countries with the most shutdowns.

Worst internet shutdown offenders in 2019

121

India

12

Venezuela

11

Yemen

8

Iraq

6

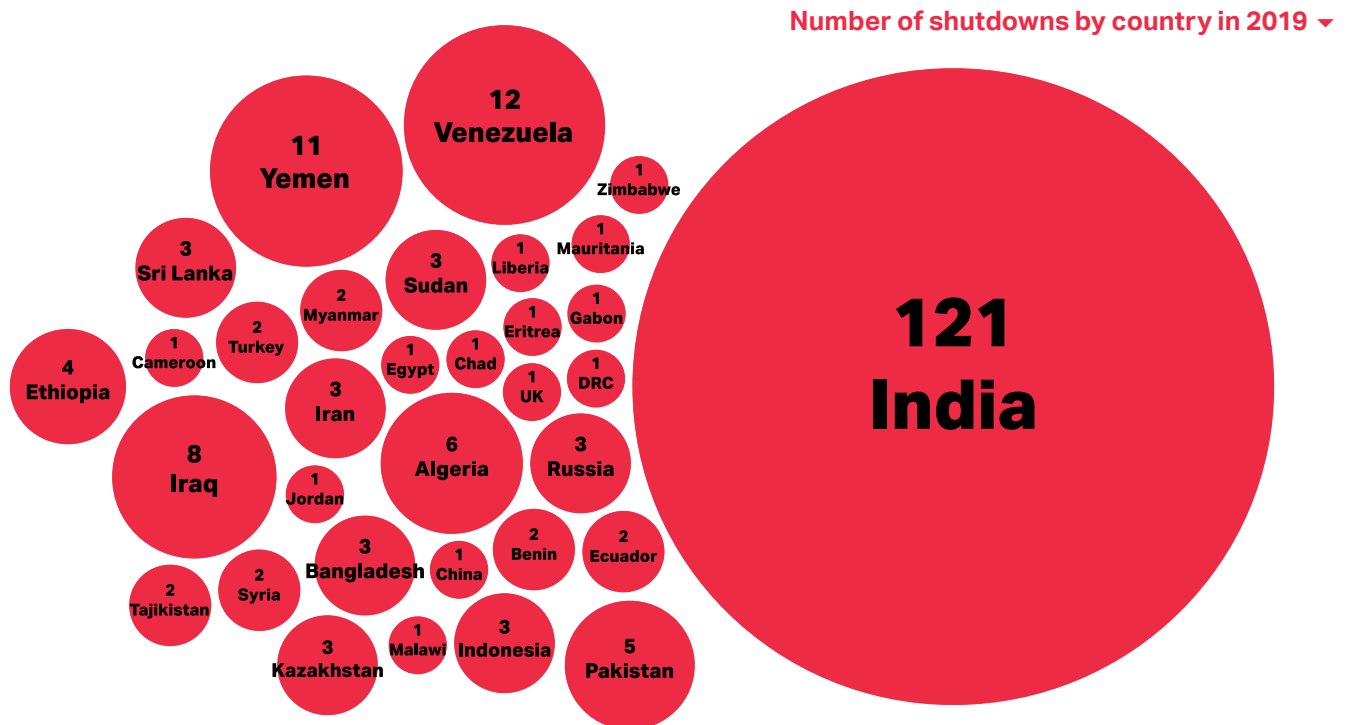
Algeria

4

Ethiopia



The world map of internet shutdowns in 2019 ▲



1 An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called “blackouts” or “kill switches.” Here’s a more technical definition developed by experts: “An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.” - Access Now (n.d.) Retrieved February 17, 2020, from <https://www.accessnow.org/keepiton/>

2 Bihar, Assam, Karnataka, and Tripura are new states that shut down the internet in 2019 but not 2018. In at least one case in Bihar, Assam, and Karnataka, authorities shut down the internet in an evident attempt to stifle dissent during protests. Times of India (2019, December 20). CAA protests: After violence in Mangaluru, mobile internet suspended in Dakshina Kannada district. Retrieved February 22, 2020, from <https://timesofindia.indiatimes.com/city/mangaluru/caa-protests-in-mangaluru-mobile-internet-suspended-in-dakshina-kannada-district/articleshow/72895087.cms>

Internet shutdowns in Africa

Compared to 2018, internet shutdowns in Africa grew by 47%. While there were 17 incidents recorded in 2018, we documented at least 25 in 2019. In addition to the increase in incidents, there was also a significant increase in the number of African countries that shut down the internet. There were 10 such countries in 2018, and at least 14 in 2019. The addition of new countries, and countries that did not disconnect the internet in 2018 or 2017, but did so in 2019, is alarming. Out of the 14 countries that shut down the internet in 2019, at least seven have either never shut down the internet or did not do so in 2018 and 2017. This includes Benin, Gabon, Eritrea, Liberia, Malawi, Mauritania, and Zimbabwe.

Internet shutdowns in Asia

Like previous years, India took the lion's share of internet shutdowns in Asia, with its record of 121 incidents, followed by Pakistan with five shutdowns in 2019. India had fewer shutdowns than it did in 2018, but some state authorities cut off networks for comparatively longer periods, such as in Jammu and Kashmir. We also saw an increasing number of states that started suspending mobile and broadband networks in India, expanding the nationwide problem. Indonesia had more shutdowns in 2019 while Pakistan had fewer, but other than that, it has been business as usual, with authorities routinely shutting down the internet for religious holidays and protests. Myanmar, China, and Tajikistan also joined the list of countries that shut down the internet in 2019. In China, the highly complex system of censorship made it extremely hard to detect and verify any instances of internet shutdowns. In the lead-up to the 30th anniversary of the Tiananmen Square protest, state-owned internet service providers (ISPs) in many provinces — including Guangdong, Shanghai, and Chongqing — reported brief internet shutdowns “due to technical problems.”³ Yet there was little transparency to reveal the reasons behind such

a massive scale of network disruption. In Tajikistan, where the internet is considered a luxury due to the high cost and low penetration rate,⁴ the authorities slowed down the already laggy internet in response to civil unrest, further deteriorating the already poor access to the internet in the country.

Internet shutdowns in Latin America

In 2019, the political turmoil people have been experiencing in Venezuela and Ecuador was reflected online. In 2018, the only country in Latin America with a documented shutdown was Nicaragua. But in 2019, there were at least 14 incidents. A full 86% of these incidents took place in Venezuela, which has a history of network-wide throttling and platform blocks.⁵ The remaining 14% of shutdowns in the region was attributed to Ecuador.

Internet shutdowns in Europe

There were at least five incidents of internet shutdowns in Europe attributed to Russia and the United Kingdom. While the United Kingdom is a new perpetrator, Russia has previously shut down the internet on numerous occasions.

Internet shutdowns in the Middle East

Yemen takes the most significant share of the internet shutdowns in the Middle East, followed by Iraq. Yemen had at least 11 confirmed cases of internet shutdowns and slowdowns in 2019. There were reports from multiple sources claiming that the number of internet shutdowns in Yemen is far higher than our documented number. Unfortunately, we were unable to verify these claims.

Amid violent protests and during scheduled school exams, there were at least eight internet shutdowns in Iraq. Iran shut down the internet at least three times, Turkey twice, and Jordan once in 2019.

³ NetEase (2019, May 13). 运营商“组团”断网，月底的流量加油包不想卖了？ Retrieved February 21, 2020, from <https://3g.163.com/dy/article/EGHRU2160527L76N.html>

⁴ Internet users comprised about 18.3% of the Tajikistan population in 2015, with the monthly subscription for fixed broadband at \$58 USD, according to the Internet Society (ISOC). Internet Society (2017, June). Tajikistan Internet Exchange Point Environment Assessment. Retrieved February 21, 2020, from <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-Tajikistan-IXP-assessment.pdf>

⁵ Pallero, J. & Arroyo, V. (2017, July 28). Connectivity problems raise red flags ahead of Venezuelan elections. Retrieved February 21, 2020, from <https://www.accessnow.org/connectivity-problems-raise-red-flags-ahead-venezuelan-elections/>

II. New trends observed in 2019

Longer shutdowns

From 2018 to 2019, the number of shutdowns lasting longer than seven days increased from 11 to 35. Chad, India, Ethiopia, Bangladesh, Myanmar, Indonesia, Democratic Republic of Congo, Eritrea, Iran, Iraq, Jordan, Kazakhstan, Mauritania, Sri Lanka, Sudan, Syria, Tajikistan, Turkey, and Zimbabwe all cut off access to the internet for more than seven days. Chad, Myanmar, and India had the longest documented shutdowns in 2019: Chad had a 472-day shutdown, Myanmar had a 248-day shutdown,⁶ and India had a 175-day shutdown. This is a clear indication of the grave situation people are facing in the blunt and extended denial of their right to access information and freely express themselves.

CHAD

Chad cut access to social media platforms, including WhatsApp, Twitter, Facebook, Instagram, and YouTube, for a staggering 472 days between 2018 and 2019. The government attempted to justify the social media blackout, stating that it was necessary for “security reasons.” However, authorities blocked access just as President Idriss Deby, who has been president of Chad since the 1990s, was pushing to stay in power until 2033.⁷

MYANMAR

Myanmar imposed the longest internet shutdown of 2019. The government first introduced the shutdown in nine townships in

Rakhine and Chin states. After 71 days, the shutdown was lifted in five of the townships, leaving four townships in a blackout. Rakhine state is where at least 500,000-600,000 Rohingya Muslims reside and where the Myanmar military is in active conflict with armed groups.⁸ At the time of publication, Myanmar has once again extended the shutdown to include at least five townships in Rakhine and Chin states.⁹

INDIA

The August 2019 internet shutdown in India was the second longest in 2019, coming alongside new legislation that fundamentally changed the political structure in Jammu and Kashmir without the consent of the people living there. Following the announcement of the changes, the government banned public gatherings in Jammu and Kashmir and put local leaders under house arrest, deployed thousands of troops,¹⁰ and shut down the internet.¹¹ After imposing a complete blackout of the internet that also uniquely included a postal blackout in Jammu and Kashmir for 175 days, Indian authorities lifted only some of the restrictions — and these restrictions have remained even after India’s Supreme Court issued a judgment that criticized the shutdown as constitutionally suspect. As of the publication of this report, residents are only allowed to access slow 2G internet connections (with 3G and 4G suspended), are blocked from accessing most social

⁶ At the time of publication, the shutdown in Myanmar was ongoing.

⁷ Woodhams, S. (2019, March 28). Chad social media ban reaches one-year mark. Retrieved February 21, 2020, from <https://africanarguments.org/2019/03/28/chad-social-media-shutdown-has-now-last-ed-a-whole-year/>

⁸ Human Rights Watch (n.d.). World Report 2019: Myanmar. Retrieved February 21, 2020, from <https://www.hrw.org/world-report/2019/country-chapters/burma>

⁹ Chau, T. (2020, February 3). Govt doubles down on internet shutdown in western Myanmar. Retrieved February 17, 2020, from <https://www.mmtimes.com/news/govt-doubles-down-internet-shutdown-western-myanmar.html>

¹⁰ Fareed, R. (2019, August 4). India imposes Kashmir lockdown, puts leaders “under house arrest.” Retrieved February 17, 2020, from <https://www.aljazeera.com/news/2019/08/india-imposes-lockdown-kashmir-puts-leaders-house-arrest-190804174841241.html>

¹¹ Human Rights Watch (2019, August 28). India: Restore Kashmir’s Internet, Phones. Retrieved February 1, 2020, from <https://www.hrw.org/news/2019/08/28/india-restore-kashmirs-internet-phones>

media platforms, and are allowed to visit only white-listed websites that are vetted by the government. (For additional details on the court ruling and current status, see Sections VI and VII of this report.)

REFUGEE CAMPS IN BANGLADESH

In 2019 the Bangladeshi government shut down mobile internet connection in refugee camps where mostly Rohingyas reside. Refugees have been barred from using SIM cards. As we prepared this report for release, the shutdown had lasted more than 168 days and was ongoing.

IRAQ

Amid massive protests against the government, in October 2019 the Iraqi government shut down the internet, switching access on and off, for more than 50 days. This restriction was imposed at a time when law enforcement agencies were accused of killing more than 23 civilians and arresting many others.¹²

More targeted geographical scope

A shutdown can be devised to target a specific neighborhood, village, region, or an entire country. One trend that was evident in 2019: governments are shutting down the internet in

a targeted fashion that bespeaks an effort to stifle the voices of specific populations, such as members of oppressed or marginalized minority groups, refugees, and others whose human rights are at risk. This trend was particularly clear in Myanmar, Bangladesh, India, and Indonesia.

One could argue that a targeted shutdown is less harmful because authorities are not taking the whole country offline. However, targeted shutdowns can be an especially obvious attempt at discrimination, exclusion, and censorship of voices speaking out against harmful government practices. This kind of harm may on its face look less damaging from the standpoint of scope. Yet these silenced voices may be absolutely crucial for alerting the public to human rights violations and abuse, and for getting help to those impacted. These kinds of targeted shutdowns, limited in their length or location, can also be more difficult to detect and verify, and are at times more easily dismissed as technical failures.

1. Bangladesh's targeted shutdowns

Bangladesh shut down the internet three times in 2019. All three of these shutdowns were targeted. The first two targeted camps inhabited by Rohingya refugees. The third targeted the border of India and Bangladesh. Authorities imposed this third shutdown on December 31, 2019, when a series of protests against the Citizenship (Amendment) Act (CAA) rocked India.¹³ The Bangladeshi government attempted to justify this shutdown as a measure for increasing national security,¹⁴ but observers speculate that it may have been intended to dissuade people from seeking refuge in Bangladesh as India's law enforcement agencies escalated their efforts to quell protests, reportedly using excessive violence.¹⁵

¹² Al Jazeera (2019, October 3). Iraq protests: Death toll rises to 20 as unrest spreads. Retrieved February 17, 2020, from <https://www.aljazeera.com/news/2019/10/iraq-imposes-curfew-baghdad-deadly-protests-191003060238724.html>

¹³ Malik, A., Mukherjee, S., & Verghese, A. (2019, December 31). In India, thousands are protesting the new citizenship law. Here are 4 things to know. Retrieved February 12, 2020, from <https://www.washingtonpost.com/politics/2019/12/31/india-thousands-are-protesting-new-citizenship-law-here-are-things-know/>

¹⁴ Khokon, S. H. (2019, December 31). Bangladesh shut down mobile services along India borders for security reasons. Retrieved February 12, 2020, from <https://www.indiatoday.in/world/story/chinese-foreign-minister-make-first-visit-abroad-germany-coronavirus-outbreak-1645795-2020-02-12>

¹⁵ Xinhua (2020, January 1). Bangladesh shuts down mobile network along India border amid fears of deportation. Retrieved February 12, 2020, from http://www.xinhuanet.com/english/2020-01/01/c_138671390.htm

2. Myanmar's targeted shutdowns

Like its neighbor Bangladesh, Myanmar targeted two regions for shutdowns: the Rakhine and Chin states, where the Myanmar military is currently in conflict with armed groups. The United Nations has accused Myanmar's military of committing genocidal attacks in these two states,¹⁶ and this shutdown took place at a time during which Burmese civil society has reported multiple human rights violations occurring there.

3. Indonesia's targeted shutdowns

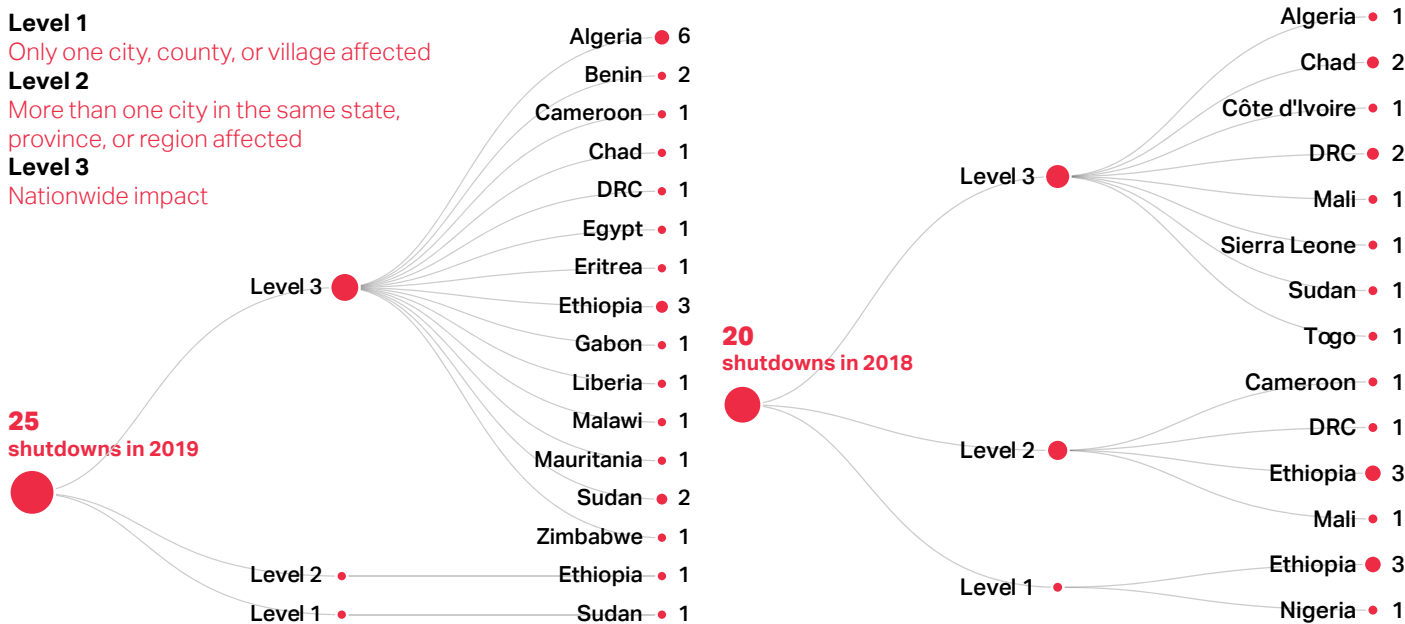
Indonesia shut down the internet at least three times in 2019. One of the shutdowns affected the whole nation, but the other two were tailored to disconnect the people of Papua. According to Human Rights Watch, a video showing the Indonesian law enforcement agencies racially abuse and discriminate against indigenous Papuan students triggered protests in multiple cities across the country.¹⁷ incident evidently led Papuans to speak out against the institutional and structural violence they have endured for many years. The government shut down the

internet and reportedly used excessive force against protesters. Indonesia had previously shut down the internet in 2018, but that shutdown affected the whole country. This year marked the first time we documented targeted shutdowns against members of minority groups in Indonesia.

Shutdowns are affecting more people in Africa

In contrast to Asia, the majority of the shutdowns in Africa were not targeted to a specific location or minority groups, instead impacting entire countries. Out of the 25 shutdowns recorded in Africa in 2019, 21 affected either an entire country or at minimum multiple regions and provinces. It is only in three cases that a shutdown targeted a specific region, city, or province. One example is a targeted shutdown that was carried out in Ethiopia.¹⁸ This indicates that shutdowns are not only growing in number but are also expanding in scope and affecting more and more people in Africa.

Affected levels of internet shutdowns in Africa



¹⁶ Office of the United Nations High Commission for Human Rights (2019, August 22). UN Fact-Finding Mission on Myanmar Calls for Justice for Victims of Sexual and Gender-based Violence. Retrieved February 12, 2020, from <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24907&LangID=E>

¹⁷ Human Rights Watch (2019, September 7). Indonesia: Investigate Deaths of Papuan Protesters. Retrieved February 13, 2020, from <https://www.hrw.org/news/2019/09/07/indonesia-investigate-deaths-papuan-protesters>

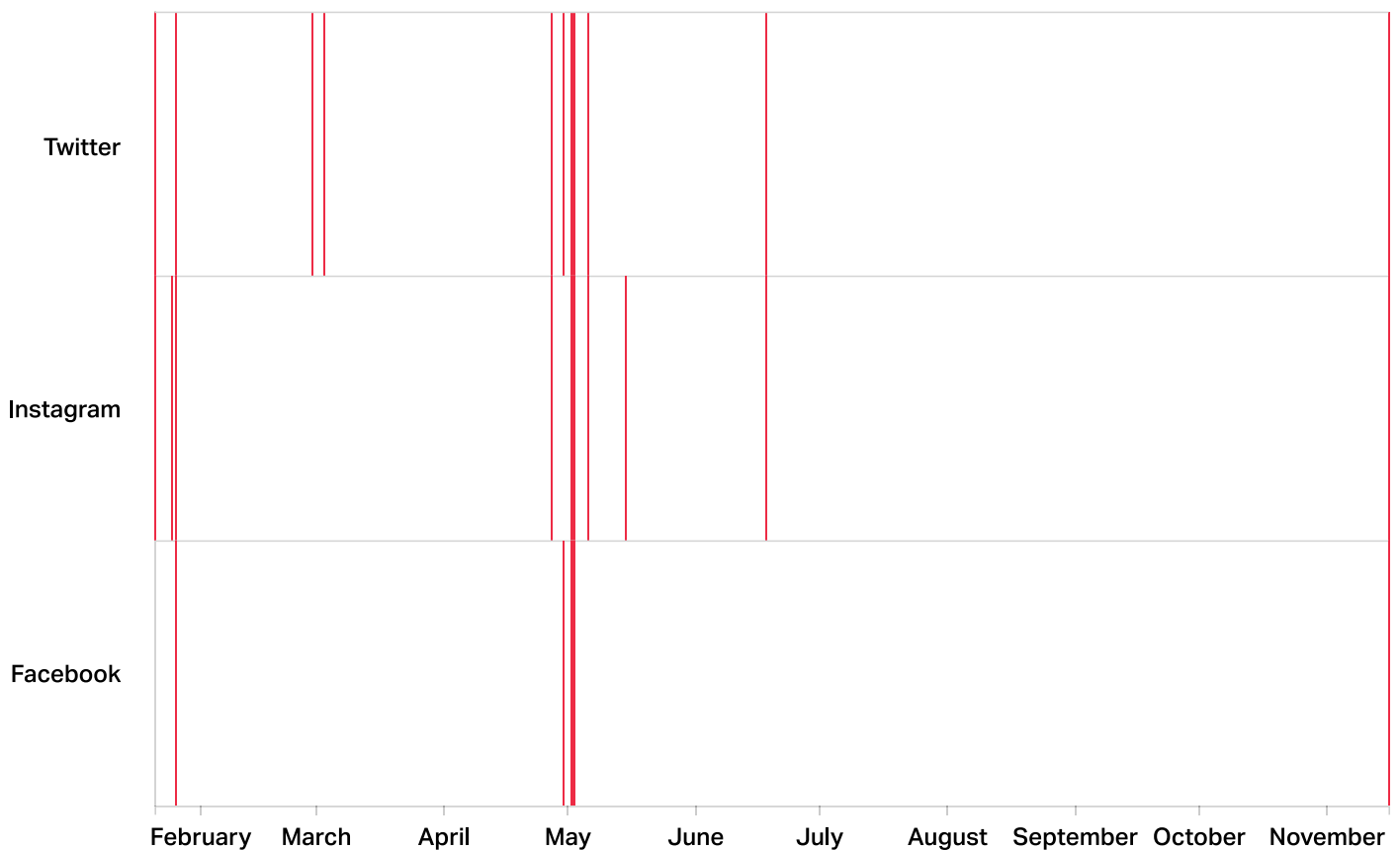
¹⁸ While Ethiopia shut down the internet numerous times in 2019, at least one shutdown targeted the Southern Nations, Nationalities and Peoples' Region (SNNPR) regional state for a sustained time frame.

Venezuela's online crisis: internet shutdowns

Two days before Juan Guaidó, the president of the National Assembly, assumed responsibility as the interim president of Venezuela,¹⁹ Nicolas Maduro's government blocked access to Twitter and Instagram on mobile and fixed-line connections. These restrictions lasted for about two hours. After Guaidó announced his claim for the presidency, online censorship ramped up: CANTV, the state-owned and dominant internet service provider, frequently blocked social media and streaming services so that people could not tune into Guaidó's speeches, National Assembly sessions, or public appearances of opposition leaders or groups.

Whenever Guaidó livestreams, the National Assembly convenes, or opposition leaders and groups develop public activities, Maduro's government blocks social media and streaming services. The minute the activity concludes, the blocking ends. The #KeepItOn coalition led by Venezuela Inteligente and others documented at least 12 such incidents in 2019, leading to Venezuela's ranking right after India for the most shutdowns in 2019. All of the incidents we documented show that the government targeted the opposition, blocking access to social media by mobile and broadband customers of CANTV and later its subsidiary Movilnet. The most commonly affected platforms were Facebook, Instagram,

Social media blocking carried out via CANTV in 2019 ▾



¹⁹ Nicolas Maduro considers this an illegitimate and illegal action, calling it an attempt to oust the government. More information about the legality can be found here: <https://www.euronews.com/2019/01/27/is-it-legal-for-juan-guaido-to-be-proclaimed-venezuela-s-interim-president>

and Twitter.²⁰ Although this tactic of targeting platforms for specific speaking events is new in Venezuela, other countries have engaged in such censorship.²¹

The internet shutdown in Venezuela was coupled with censorship of traditional media and other attempts to disrupt anonymous browsing. In line with their previous ill-chosen actions, CANTV and other ISPs blocked independent media web pages²² in 2019, repeating what CANTV has done in previous years, when it blocked independent media²³ and tools for circumventing blocks, such as the Tor browser.²⁴ The majority of those web pages remain blocked as of the publication of this report.. Having access to independent media through the internet is important in Venezuela, as the government has closed traditional media and arrested journalists and opposition leaders, and it was one of the few remaining pathways to escape from censorship.

Moreover, the amendment of the law on Social Responsibility in Radio, Television and Electronic Media (2010), the Decree of the State of Exception and Economic Emergency

(2017), and the Constitutional Law against Hate, for Peaceful Coexistence and Tolerance (2017) constitute a legal framework²⁵ that allows online censorship. Nevertheless, the Maduro government has never publicly acknowledged nor used this legal framework to justify the targeted blockings of platforms and independent media web pages. CANTV conducts most of the blocking and filtering without further explanation. Some reports also implicate internet service providers like Movistar, Digitel, and InterClient in blocking and filtering social media.

What is clear to observers is that these tactics are leveraged to control the free flow of information, deny people their right to access information and free expression, and interfere with people's ability to organize, online or off.

Venezuela's online crisis did not start in 2019 nor with the rise of Guaidó. This crisis is getting worse day after day due to the lack of maintenance and development of the CANTV network²⁶ and the electricity²⁷ system that might be one of the causes of the frequent power blackouts.

20 YouTube and Periscope were also a target. Access Now only documents mobile apps that enable two-way communication between users.

21 For instance, in 2018, Kazakhstan throttled social media when opposition leaders live-streamed events.

22 During the visit of Michelle Bachelet, U.N. High Commissioner for Human Rights, there were many websites that stayed blocked. Azpúrua, A. (2019, June 21). Censura en #InternetVE no se de tiene por visita de Bachelet. Retrieved February 17, 2020, from https://vesinfiltro.com/noticias/la_censura_no_se_detiene_por_visita_de_bachelet/

23 More information about blockings in previous years here: Azpúrua, A., Chirinos, M., Evdokimov, L., & Xynou, M. (2018, August 16). A study by Venezuela Inteligente / VESinFiltro, IPYS Venezuela, and OONI on internet blocks in Venezuela. Retrieved February 21, 2020, from https://vesinfiltro.com/noticias/state_of_internet_censorship_2018-08-16/

24 Access Now (2018, June 28). Venezuela blocks access to the Tor network. Retrieved February 21, 2020, from <https://www.accessnow.org/venezuela-blocks-tor/>

25 At the beginning of 2019, news leaked that the government was about to introduce a cybersecurity bill that proposed, among other things, the dangerous concept of "content security" to legitimize tools, policies, rules, and "preventive actions" to "counteract hate" on the internet. More information can be found here: Arroyo, V. (2019, January 22). A bill in Venezuela seeks to give the government absolute control over the internet. Retrieved February 21, 2020, from <https://www.accessnow.org/a-bill-in-venezuela-seeks-to-give-the-government-absolute-control-over-the-internet/>

26 Álvarez, J. (2020, January 30). [Reportaje Especial] CANTV en las ruinas. Entérese por qué la principal empresa de telefonía del país no brinda respuesta a las averías. Retrieved February 17, 2020, from <https://puntodecorte.com/cantv-en-las-ruinas/>

27 Diaz, M. (2016, June 8). In Venezuela, Electrical Shortages Limit Basic Communication — and Free Expression. Retrieved February 17, 2020, from <https://advox.globalvoices.org/2016/06/08/in-venezuela-electrical-shortages-limit-basic-communication-and-free-expression/>

III. Networks, services, and communications affected by internet shutdowns

Services affected in 2019

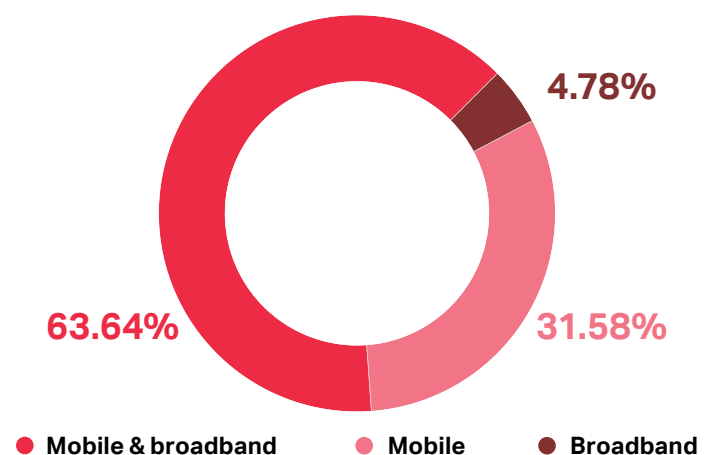
Whether a shutdown is aimed at quelling protests, stopping cheating during exams, or influencing an election, authorities will often target specific services. In some contexts, a government will impose a shutdown of mobile data, and in others will block both mobile data and fixed-line connections. A shutdown can block social media and impact only those trying to connect via mobile, or throttle access to only specific services. This kind of internet shutdown is difficult to identify, verify, and document. For instance, a small village might be denied access to social media through mobile data, but might still have access through fixed lines. If one does not measure and document connectivity and access through each access point, on each telecom, and each internet service provider, it is hard to document each case.

The #KeepItOn coalition classifies network disruptions into internet shutdowns and throttling.²⁸ Globally, out of the 213 network disruptions documented in 2019, at least 196 were shutdowns,²⁹ 10 were throttling accompanied with shutdowns, four were just throttling, and three were unknown. Out of the 196 shutdowns, 63 targeted mobile data and 123 targeted both mobile and fixed-line connections. At least 38 incidents affected only service-based platforms such as Facebook, Twitter, Instagram, WhatsApp, and other social media services. It is common for countries first to block access to social media, then to impose a complete blackout of internet services. There

were at least 10 such cases in 2019. When governments cut access to social media, victims of the shutdown tend to turn to virtual private networks (VPNs) to circumvent blocking. In some cases, governments then move to cut access to the internet entirely. Benin, Zimbabwe, Gabon, and India have been perpetrators of this kind of progressive restriction.

In 2019, there were 10 cases where only fixed-line connections were shut down: one in Eritrea, eight in Yemen, and one in the United Kingdom. The United Kingdom cut fixed-line WiFi connection in an underground transportation system in an attempt to “prevent and deter serious disruption” by climate change protesters,³⁰ while Eritrea cut access to broadband internet in anticipation of protests. Eritrea did not shut down mobile data because people are not allowed to use mobile internet anyway, even in the rare cases when they have SIM cards.³¹

Affected networks in 2019 ▾



²⁸ Throttling in the context of internet shutdowns is understood to mean the intentional slowing of an internet service by an internet service provider.

²⁹ Shutdown in this context is understood to mean the intentional disruption of internet connection and/or mobile apps that enable two-way communication.

³⁰ Vincent, J. (2019, April 17). UK police shut off Wi-Fi in London Tube stations to deter climate protesters. Retrieved February 14, 2020, from <https://www.theverge.com/2019/4/17/18411820/london-underground-tube-wi-fi-down-shut-off-protests-extinction-rebellion>

³¹ BBC News (2019, October 15). Where ATMs are unknown and SIM cards are like gold dust. Retrieved February 13, 2020, from <https://www.bbc.com/news/world-africa-49727573>

If you can't shut them off, slow them down!

There were at least 14 cases of throttling in 2019: as previously stated, 10 of these incidents were followed by complete blackout, while the remaining four were throttling alone. Jordan, Ecuador, Zimbabwe, India, Benin, China, Tajikistan, Kazakhstan, and Bangladesh all throttled either internet services as a whole or specific services in 2019. For instance, Jordan and Ecuador each throttled social media platforms. The Jordan Open Source Association in collaboration with the Open Observatory of Network Interference (OONI) documented Jordan's attempt to throttle Facebook Live for over 21 days in an evident effort to quell anti-austerity protests.³² Ecuador slowed down access to Facebook, Twitter, and WhatsApp in an evident effort to deter protesters from denouncing austerity measures

Other countries coupled throttling with shutdowns. For instance, Kazakhstan and Tajikistan first throttled social media for a few hours and then resorted to completely blocking Instagram, Twitter, and Facebook. Benin and Zimbabwe throttled social media platforms, then blocked them, and finally cut access to the internet entirely.

Social media blocking

In 2019 people around the world used social media platforms to organize grassroots movements, from Sudan to Venezuela and beyond. These same platforms are of course also leveraged to spread false information, target activists and journalists, and fan hate speech. Yet as two-way communications platforms, they remain an avenue for empowering users, and governments have made numerous attempts to throttle or block access to these services.³³

³² Jordan Open Source Association & Open Observatory of Network Interference (n.d.). Technical Report | Measuring Facebook Live-Streaming Interference during Protests in Jordan. Retrieved February 17, 2020, from <https://jordanopensource.org/technical-report/>

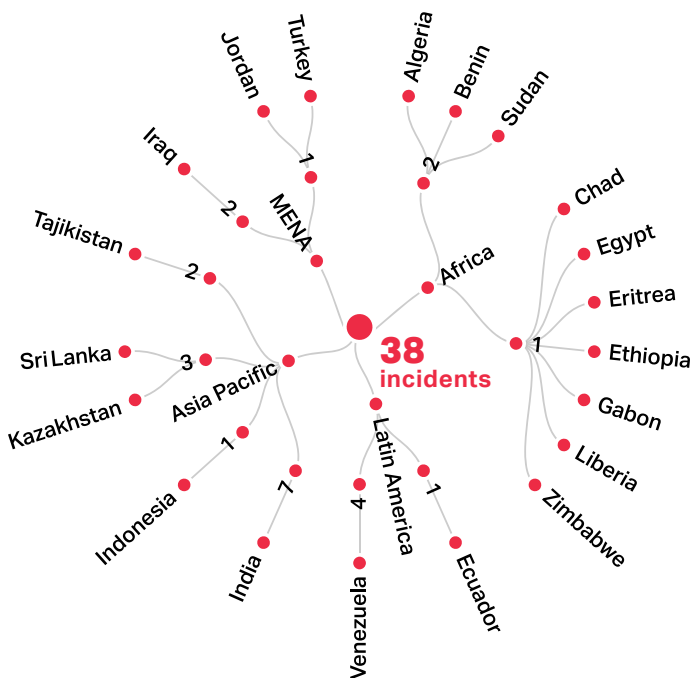
³³ Please note that blocking is reported by users and the measurement community, so there may be false positives. For accuracy in documenting shutdowns, social media platforms should be transparent about targeted blocking and throttling of their services.

³⁴ Please note that this number might change once Facebook publishes its internet disruption report accessible via: <https://transparency.facebook.com/internet-disruptions>

³⁵ Please note that this number might change if Twitter publishes reports detailing attempts to block and slow down services.

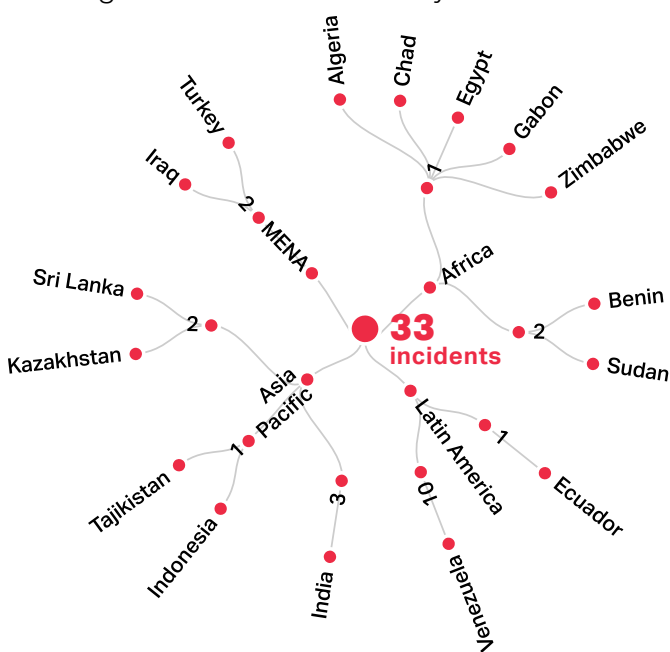
1. Facebook

There were at least 38 user-reported incidents where Facebook was blocked.³⁴



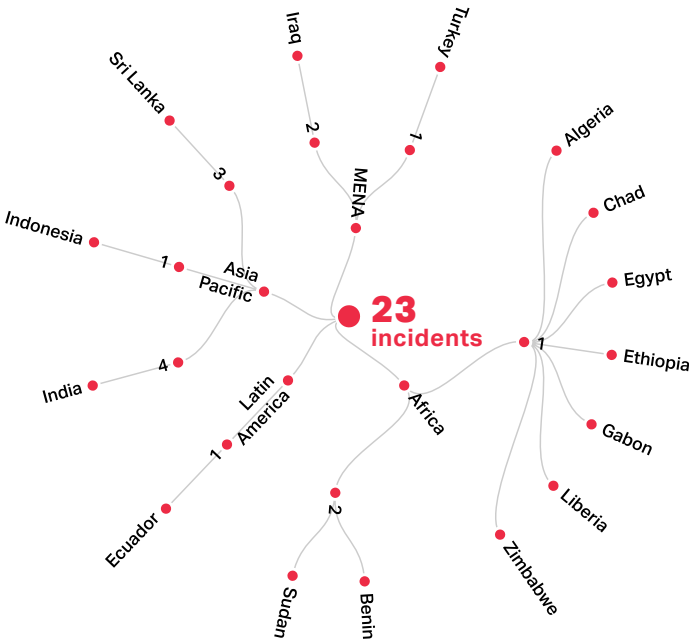
2. Twitter

There were at least 33 user reported incidents where governments intentionally blocked Twitter.³⁵



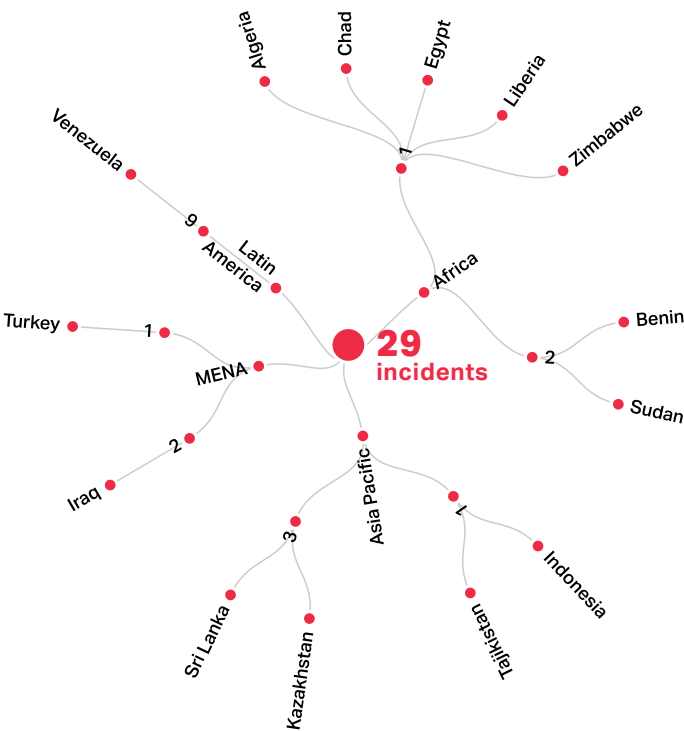
3. WhatsApp

There were at least 23 user-reported incidents of WhatsApp blocking.³⁶



4. Instagram

There were at least 29 incidents of user-reported Instagram blocking.³⁷

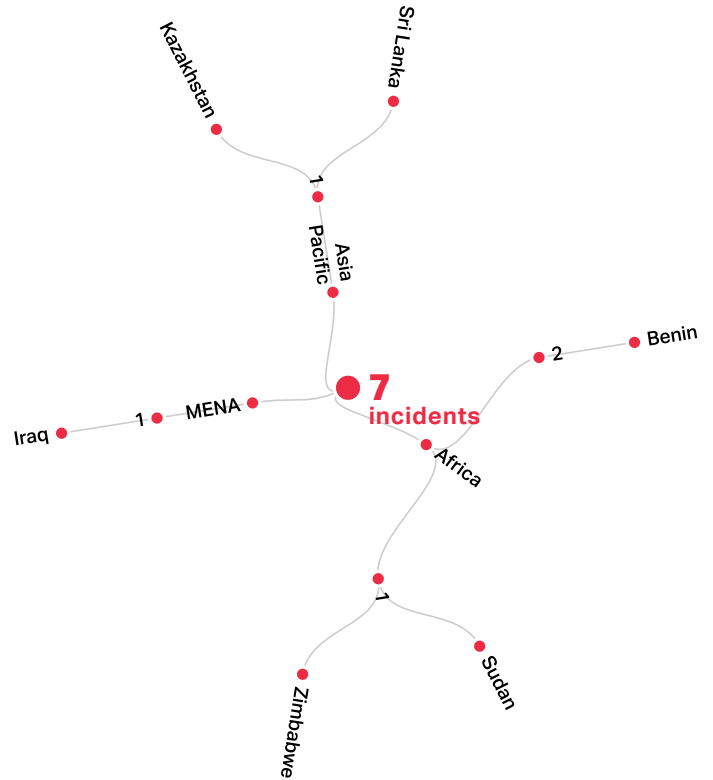


³⁶ Please note that this number might change if WhatsApp publishes details about attempts to block and throttle access to the app.

³⁷ Please note that this number might change if Instagram publishes details about attempts to filter and slow down access to the app.

5. Telegram

There were at least seven user-reported incidents of blocking on Telegram. It is very likely that there were many more incidents of such blocks, but Telegram does not publish transparency reports or information on internet disruptions, so it is difficult to verify and document these events.



IV. What do the governments say?

Do governments ever acknowledge internet shutdowns?

In 2018, governments acknowledged only 81 internet shutdowns, but in 2019 they acknowledged at least 116. These acknowledgements came in a variety of forms: through a memo, press briefing, 280 characters on Twitter, or via documents forced into the light through a lawsuit or request for public

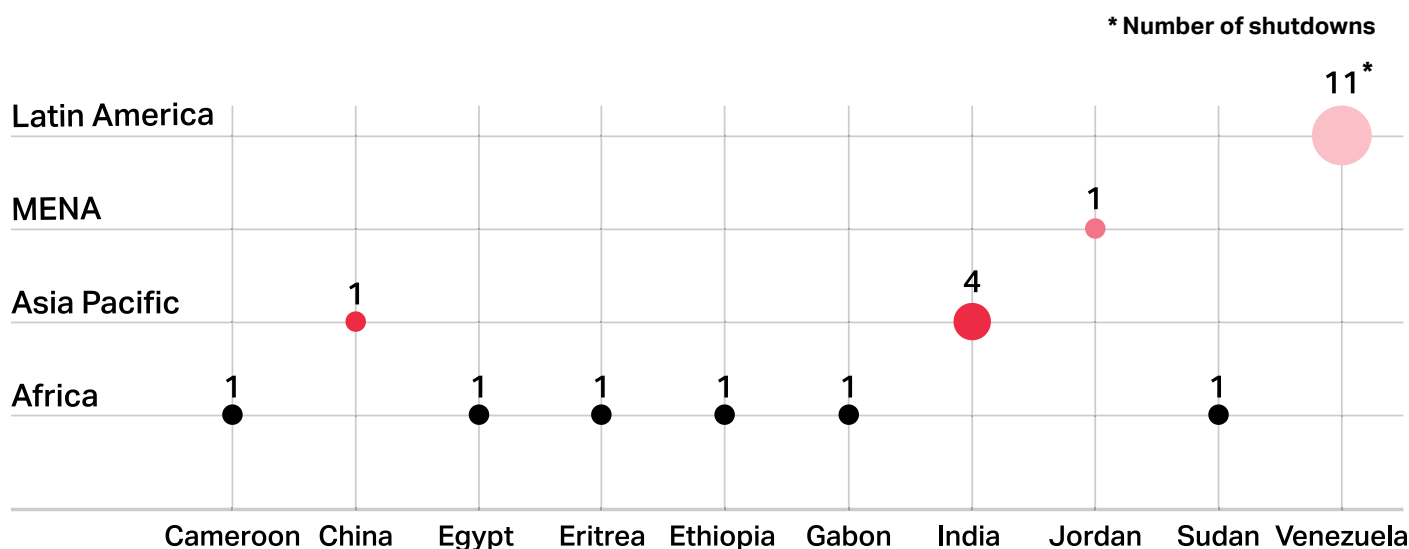
access to information. When the Ethiopian Prime Minister acknowledged his order to shut down the internet, he reportedly said, "as long as it is deemed necessary to save lives and prevent property damages, the internet would be closed permanently, let alone for a week...it is neither water nor air."³⁸

There were at least 10 governments that completely ignored requests for confirmation that they had purposely cut access to the internet.

Number of governments that acknowledged internet shutdowns ▾



10 governments did not acknowledge internet shutdowns in 2019 ▾



³⁸ AfricaNews (2019, August 1). Ethiopia will cut the internet as and when, 'it's neither water nor air' - PM Abiy. Retrieved February 14, 2020, from <https://www.africanews.com/2019/08/02/ethiopia-will-cut-internet-as-and-when-it-s-neither-water-nor-air-pm-abiy/>

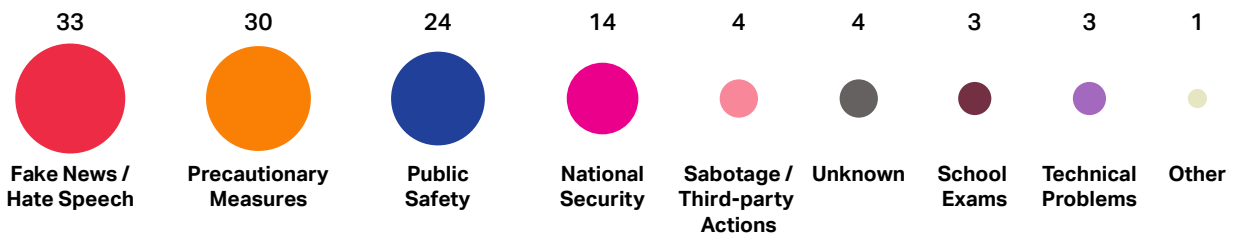
How did governments justify shutdowns in 2019?

When governments acknowledge shutdowns, they attempt to justify them. The most common official justification for ordering shutdowns in 2019 was “fighting fake news, hate speech, or content promoting violence,” followed by “precautionary measures,”³⁹ public safety, national security, third-party actions, school exams, and technical problems.

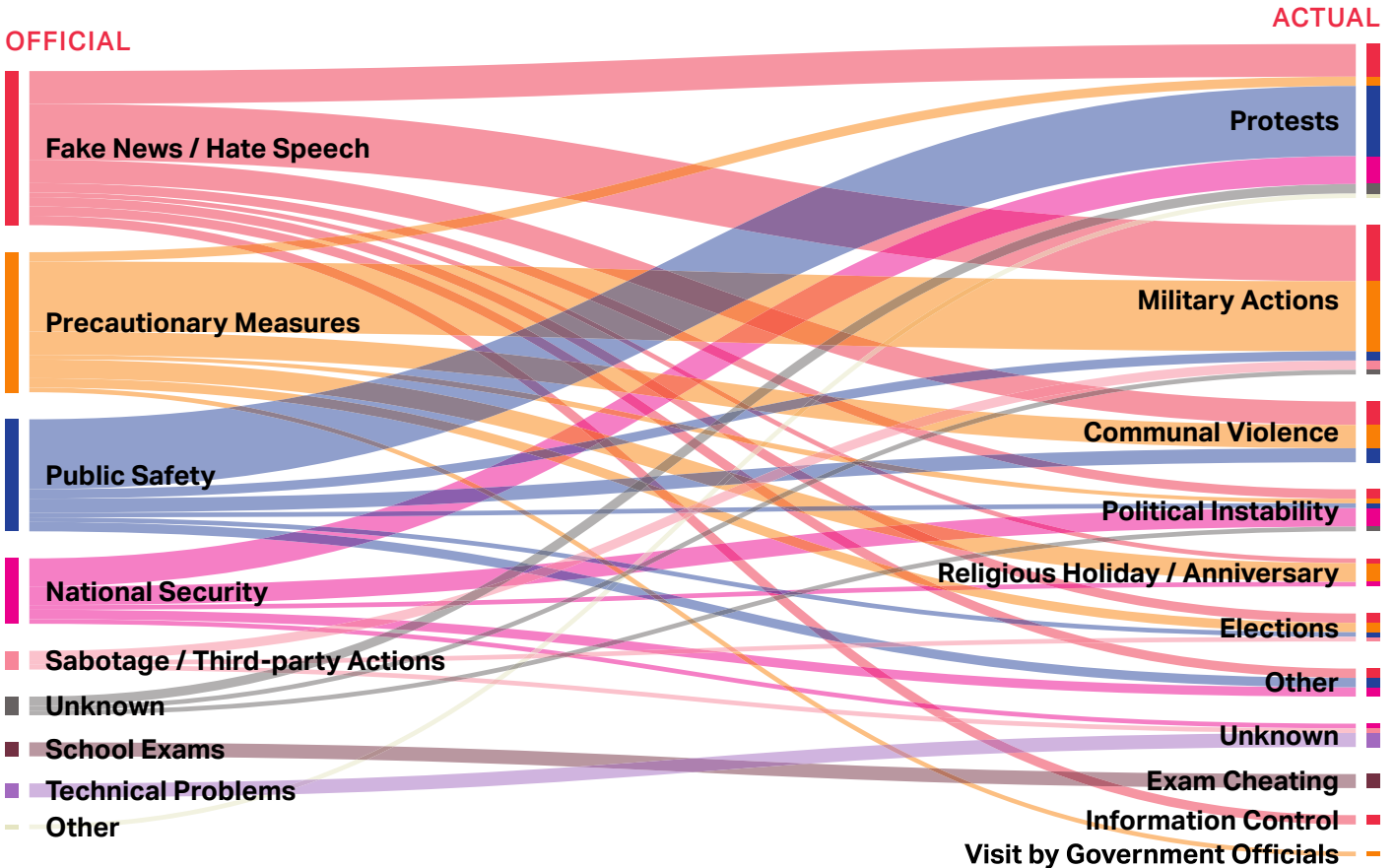
While governments justify shutdowns for a variety of reasons, their justifications rarely match what observers conclude is the actual

cause. In 2019, the most commonly observed causes were protests, military actions (mostly in India), communal violence, political instability, religious holidays or anniversaries, and elections. In examining the data from 2019, it is evident that when a government says it is cutting access to restore “public safety,” in reality it could mean the government anticipates protests and may be attempting to disrupt people’s ability to organize and speak out, online or off. Similarly, a government claim that a shutdown is necessary to fight “fake news,” hate speech, or incendiary content could be an attempt to hide its efforts to control the flow of information during periods of political instability or elections.

Justifications used by governments that ordered shutdowns in 2019



Justifications vs. actual causes



³⁹ “Precautionary measures” are almost always used by the Indian government to justify shutting down the internet in situations of military action, such as in Jammu and Kashmir.

V. Elections, protests, and shutdowns: What we know from 2019

Elections and shutdowns

In Sri Lanka, Benin, Senegal, Spain, Bolivia, and other countries around the world, millions of people headed to the polling stations to elect their leaders in 2019. Some of these elections have resulted in a peaceful transfer of power. Others have been marred by violence and had their legitimacy undermined by internet shutdowns.

The internet is an essential tool for free and fair elections. Voters around the world depend on the internet to find information about candidates, polling stations, election processes, and election results. As much as voters use the internet to exercise their democratic rights, they also use the internet to expose election fraud, voter intimidation, and other malpractices before, during, and after elections. Meanwhile, candidates use the internet to campaign and convince voters to their side. Election authorities depend on the internet to conduct elections, transmit election results, educate voters, and announce election outcomes.

Given the key role the internet plays during elections, any attempt to disconnect or slow down internet connections, or to block and filter social media platforms, will affect essential election processes, and in certain circumstances, it will also affect election results.

In 2019, the #KeepItOn campaign documented internet shutdowns during election periods in Benin, India, the Democratic Republic of Congo, Malawi, Mauritania, Indonesia, and Kazakhstan.

BENIN

Benin shut down the internet during parliamentary elections in April and May 2019. This was perhaps the most alarming

and unexpected election-related shutdown of the year. Benin has had a multiparty system since the 1990s, before many of its neighbors. Although the democratic situation in Benin was deteriorating in 2019, many in civil society were not expecting to see Benin shut down the internet during elections.

There were two shutdowns. The first was on election day. The government first throttled, then cut access to social media for a few hours. When people resorted to using circumvention tools like VPNs, the government then blocked access and imposed a blanket internet shutdown, taking the entire country off the grid during one of the most important days for its aspiring democracy. Shortly after the internet was restored, the government tweeted “inviting” citizens to verify information through its official channels and warned against sharing “fake news.”⁴⁰ The second shutdown took place a few days after the election, without any clear justification.

This was not the first time the government in Benin had attempted to interfere with people’s access to the internet. In 2018, the government had introduced a bill to tax users of social media platforms. Due to protests and grassroots organizing, the government scrapped the bill one day after it was introduced. When unable to levy taxes, the government introduced higher prices for mobile data.⁴¹ Benin’s attempt to tax social media and extort more revenue with higher data prices indicates a lack of regard for ensuring the internet is accessible to all of its citizens, and puts us on notice for future restrictions to access like the throttling and blocking we saw in 2019.

⁴⁰ Gouvernement du Bénin (2019, May 2). Retrieved February 14, 2020, from <https://twitter.com/gouvbenin/status/1123696637258424320>

⁴¹ Internet Without Borders (2019, April 28). Internet shutdown and Democratic Backsliding in Benin. Retrieved February 14, 2020, from <https://internetwithoutborders.org/internet-shutdown-and-democratic-backsliding-in-benin/>

SENEGAL AND NIGERIA

Unlike in Benin, civil society in other countries expected authorities to shut down the internet during elections. In Senegal and Nigeria, civil society lobbied their respective governments to keep the internet on. Each country responded and set a positive example by refraining from any interference with the internet during elections.

Senegal held presidential elections in 2019, and like many people around the world, members of Senegalese civil society feared the government would, at minimum, block social media during the elections and, at worst, cut internet access entirely. Encouraged by the efforts of other similar movements to prevent shutdowns in other countries, they engaged in advocacy for transparency and accountability for shutdowns⁴² and succeeded in forcing the communications authority to openly declare, a few days before the election, its commitment to keeping the internet open and secure — before, during, and after elections.⁴³

Activists in Nigeria followed the footsteps of their counterparts in Senegal, and also succeeded. Even though many thought Nigeria would shut down the internet during elections, the communications authority of the most populous state in Africa instead publicly declared its commitment to keep the

internet on during elections,⁴⁴ and followed through with that commitment.

Protests and internet shutdowns

From Bolivia and Venezuela, to Sudan, Iran, India,⁴⁵ and beyond, 2019 was a turbulent year. While millions of people around the world took to the streets in protests to demand change and oust dictators, governments were busy shutting down the internet in evident attempts to silence dissent and thwart the capacity of protesters to organize and assemble. The #KeptOn coalition recorded at least 65 internet shutdowns during protests in 2019. The most notable are in Sudan, Iraq, Iran, Venezuela, Zimbabwe, Algeria, India, and Indonesia.

SUDAN: #IAMTHESUDANREVOLUTION

While governments claim that internet shutdowns increase public safety,⁴⁶ they in fact enable human rights violations to take place in the dark. During the internet shutdowns in Sudan in June 2019, several reports indicated that more than 100 people

⁴² APA News (2019, February 21). Senegal CSOs demand 'secured' internet on polling day, beyond. Retrieved February 21, 2020, from <http://apanews.net/en/pays/senegal/news/senegal-csos-demand-secured-internet-on-polling-day-beyond>

⁴³ ASUTIC (2019, February 23). Retrieved February 22, 2020, from <https://twitter.com/asuticsenegal/status/1099383677421842432>

⁴⁴ Taye, B. (2019, February 14). Nigeria's coming election: countering the threat of internet shutdowns and online censorship. Retrieved February 21, 2020, from <https://www.accessnow.org/nigeria-election-countering-internet-shutdowns/>

⁴⁵ Access Now (2019, December 20). With shutdowns in major cities to silence protests, India tries to black out democracy. Retrieved February 23, 2020, from <https://www.accessnow.org/with-shutdowns-in-major-cities-to-silence-protests-india-tries-to-black-out-democracy/>

⁴⁶ AfricaNews (2019, August 1). Ethiopia will cut internet as and when, 'it's neither water nor air' - PM Abiy. Retrieved February 14, 2020, from <https://www.africanews.com/2019/08/02/ethiopia-will-cut-internet-as-and-when-it-s-neither-water-nor-air-pm-abiy/>

were killed,⁴⁷ over 700 injured, and at least 70 raped.⁴⁸ This was not the first time Sudan had shut down the internet, but this round was different: this time, the shutdown was evidently introduced to deter protesters from livestreaming the reported systematic and organized killings and looting by the Transitional Military Council (TMC). Just before mobile internet was shut down, the TMC, which had been negotiating with opposition groups to set up a transitional civilian government, withdrew from the negotiations and sent in the Janjaweed militia in a reported murderous attack on peaceful protesters.⁴⁹

IRAN: #IRANPROTESTS

The Iranian government's decision to hike fuel prices by 50%, after years of political and economic instability and threats to human rights, is what evidently drove Iranians across the country into the streets to demand change. According to Amnesty International, at least 300 protesters were killed, many were injured, and more than a thousand were arrested.⁵⁰ Iran plunged the whole country into darkness, with a comprehensive shutdown that was very difficult for Iranians to circumvent. That made what was already

an inherently disproportionate interference with Iranians' human rights even more harmful and dangerous.

IRAQ: #IRAQPROTESTS #INSM_IQ

As mass anti-government protests began in Iraq, thousands protested rising unemployment, failing public services including long power outages, and government corruption.⁵¹ The security forces responded by killing 100 people and injuring more than 800 protesters, according to international media.⁵² The wave of protests were sparked in Tahrir Square, Baghdad and spread nationwide, taking place in at least seven other provinces. Within just a few hours of the initial protests, Iraqi authorities blocked Facebook, Twitter, WhatsApp, Instagram, and other social and messaging apps, multiple times. As the situation escalated, Iraqi authorities imposed a near-total internet shutdown. It also shut down government offices, introduced a curfew in several cities, deployed thousands of heavily armed security forces, arrested hundreds of people, and engaged in conflict for an extended period of time, reportedly resulting in protester deaths.⁵³

47 Al Jazeera (2019, June 10). Sudan: 'Several killed' on first day of civil disobedience. Retrieved February 14, 2020, from <https://www.aljazeera.com/news/2019/06/sudan-police-fire-tear-gas-civil-disobedience-campaign-starts-190609084804785.html>

48 Salih, Z. M. & Burke, J. (2019, June 11). Sudanese doctors say dozens of people raped during sit-in attack. Retrieved February 14, 2020, from <https://www.theguardian.com/world/2019/jun/11/sudan-troops-protesters-attack-sit-in-rape-khartoum-doctors-report>

49 Ibid.

50 Swart, M. (2019, December 17). 'Vicious crackdown': Iran protest death toll at 304, Amnesty says. Retrieved February 14, 2020, from <https://www.aljazeera.com/news/2019/12/crackdown-iran-protest-death-toll-304-amnesty-191216091026260.html>

51 Mansour, R. (2019, October 7). Iraq protests: What's behind the anger? Retrieved February 14, 2020, from <https://www.bbc.com/news/world-middle-east-49960677>

52 Alkshali, H., Tawfeeq, M., & Qiblawi, T. (2019, October 5). Death toll rises to 93 in Iraq amid ongoing protests. Retrieved February 17, 2020, from <https://edition.cnn.com/2019/10/03/middleeast/iraq-economic-protests-intl/index.html>

53 Chulov, M. (2019, October 4). Internet blackout in Iraq as death toll from violent protests rises. Retrieved February 14, 2020, from <https://www.theguardian.com/world/2019/oct/03/internet-down-across-iraq-third-day-protests>

VI. Judges raise the gavel to #KeepItOn around the world

Access Now has been tracking legal actions to challenge shutdowns since 2015, documenting petitions, lawsuits, appeals, and other court actions against telecommunications companies (telcos) and governments.⁵⁴ In our most recent documentation dated December 2019,⁵⁵ we recorded 19 cases in 12 countries, from Russia to India, Cameroon, Indonesia, and elsewhere. In 2019, while the number of internet shutdowns appeared to increase, so did the legal challenges aimed at stopping them.

From 2015 to 2017, we recorded only a handful of legal cases. But in 2018, we added five cases, and in the first half of 2019 alone, we added another five. As of the publication of this report, cases are pending in the Economic Community of West African States (ECOWAS) Community Court, where Amnesty International West Africa and others are suing Togo for its 2017 shutdown, and at the African Commission regarding disruptions in Cameroon. In India, multiple petitions were launched regarding the shutdown in Jammu and Kashmir, with mixed success. Petitions were also launched across high courts in different Indian states challenging the shutdowns ordered following nation-wide protests against the Citizenship (Amendment) Act and proposed National Register of Citizens. Not only are there more legal challenges, we are also seeing more victories — at least procedural wins, if not always on the merits — such as ones in Zimbabwe, Sudan, and India. That’s heartening, given the many risks and challenges of pursuing legal action on shutdowns around the world.

It is frequently lawyers, often independent practitioners without many resources or protections, who are at the front lines of this battle. The cases challenging shutdowns are almost always brought with the support of civil society

organizations seeking to defend constitutional and consumer rights. However, they should not have to fight alone. Telcos have the opportunity and responsibility to demonstrate respect for the human rights of shutdown victims, and they can use their legal arms and telecom industry associations to resist government demands and bring more transparency to the orders, which often exceed a state’s legal authority. Institutions from internet platforms to bar associations and technical bodies all have roles to play in advancing norms and standards that can inform courts and assist them in providing meaningful remedy.

INDIA

A 2019 case against the months-long shutdown in Kashmir made its way to the Indian Supreme Court. In January 2020, the highest court in the country ruled on the merits, declaring that shutdowns interfere with the fundamental right to freedom of expression and the right to life and liberty, that shutdown orders must be publicly available, and that indefinite shutdowns are unconstitutional, among other positive findings. The court also recommended that the existing Network Suspension Rules of 2017 be modified. However, the ruling failed to provide immediate relief to those suffering under the Kashmir blackout, with authorities choosing to continue the disruption of internet access by keeping 3G and 4G services blocked, banning access to social media sites and maintaining a “whitelist” of sites that residents in the affected areas could access.⁵⁶ The intervention was filed and argued by senior advocate Vrinda Grover

⁵⁴ Micek, P. & Libbey, M. (2019, September 25). Judges raise the gavel to #KeepItOn around the world. Retrieved February 21, 2020, from <https://www.accessnow.org/judges-raise-the-gavel-to-keepiton-around-the-world/>

⁵⁵ Access Now (2019, December). Shutdown Lawsuit Monitor (SLaM) 2019. Retrieved February 21, 2020, from https://www.accessnow.org/shutdown-lawsuit-monitor-slam_-tracking-legal-actions-around-internet-shutdowns-confirmed-2/

⁵⁶ Internet Freedom Foundation (2020, January 10). SC’s Kashmir communication shutdown judgement is just the beginning of a long uphill campaign. Retrieved February 21, 2020, from <https://internetfreedom.in/scs-judgement-on-kashmir-communication-is-just-the-beginning/>

on behalf of Anuradha Bhasin, editor of the Kashmir Times, and was supported by interventions from the Foundation for Media Professionals and the Indian Journalists Union, with the latter supported by lawyers from the non-profit Internet Freedom Foundation and other pro bono counsel.

As protests over India's Citizenship (Amendment) Bill erupted in more than 10 districts in Assam, the government imposed internet shutdowns. After advocates took the Assam state government to court over the network disruption, the Gauhati High Court ordered immediate restoration of internet access in all districts of Assam, noting that "[n]o material is placed by the State to demonstrate and satisfy this Court that there exists, as on date, disruptions on the life of the citizens of the State with incidents of violence or deteriorating law and order situation, which would not permit relaxation of mobile Internet services."⁵⁷ This progressive decision from the Gauhati court forced the state authority to restore internet connectivity.

On September 19, 2019, the high court in the Indian state of Kerala found the "Right to Internet Access" to be a fundamental right, according to the Delhi-based not-for-profit organization SFLC.in (Software Freedom Law Centre, India).⁵⁸ The court declared that the right to have access to the internet becomes a part of the right to education as well as the right to privacy under the Constitution of India. The petition was filed by Faheema Shirin, a hostel resident and student of Sree Narayana College, Chelanur, Kozhikode against the discriminatory girls' hostel rules, which banned the use of mobile phones at night. Shirin was expelled from the hostel for protesting against the rules, before filing the lawsuit. SFLC.in intervened in the matter.

ZIMBABWE

A case in Zimbabwe demonstrates that, in shutdown litigation, technical legal questions such as standing, statutory construction, and procedure can guide a court just as much as human rights arguments. In January 2019, advocate Eric Matinenga, representing Zimbabwe Lawyers for Human Rights and MISA Zimbabwe, brought a lawsuit against the state. In its decision, the court ruled that the Minister of State in the President's Office Responsible for National Security "does not have the authority to issue any directives in terms of the Interception of Communications Act," making the order that led to the Zimbabwean internet shutdown illegal and without effect. According to Matinenga, the ruling is narrow, as it is based on "preliminary points" and procedure, rather than substantive arguments.⁵⁹

SUDAN

Even in cases where the internet is disrupted during a turbulent period, relying on the rule of law and persistence in the courts can be effective in restoring access, given that extreme care must be taken to protect the safety of those involved in the litigation. In Sudan, Abdelazeem Hassan took telco company Zain to court just a few weeks after the internet was first disrupted. He won the case, but because he filed in a personal capacity, Zain restored access only to Hassan's personal devices. Not satisfied with this result, he returned to court to challenge the other two companies behind the shutdown, MTN and Sudatel. This time, the court didn't leave that loophole open. For the first time in five weeks, the internet was restored to all of Sudan.⁶⁰

⁵⁷ Sengupta, S. (2019, December 22). How Gauhati HC Order on Lifting Ban Brings Hope in the Land of Maximum Internet Shutdowns. Retrieved February 23, 2020, from <https://www.news18.com/news/india/how-gauhati-hc-order-on-lifting-ban-brings-hope-in-the-land-of-maximum-internet-shutdowns-2431619.html>

⁵⁸ SFLC.in (2019, September 20). Kerala High Court Declares 'Right to Access Internet' as a Fundamental Right. Retrieved February 21, 2020, from <https://sflc.in/kerala-high-court-declares-right-access-internet-fundamental-right>

⁵⁹ Access Now (2019, September 25). Judges raise the gavel to #KeepItOn around the world. Retrieved February 21, 2020, from <https://www.accessnow.org/judges-raise-the-gavel-to-keepiton-around-the-world/>

⁶⁰ Buelgasim, F. & Magdy, S. (2019, July 10). Sudan activists say internet restored after crackdown. Retrieved February 21, 2020, from <https://apnews.com/e1541a09119e49d1894e8708c5683988>

VII. Business as usual — India tops the list of countries ordering the most shutdowns in 2019

The #KeptOn campaign documented at least 121 internet shutdowns in India in 2019. The number is lower than it was in 2018, but this is not necessarily positive. We saw extended shutdowns, instead of the pattern of shorter disruptions we observed in 2018. India imposed a complete blackout in the Jammu and Kashmir that lasted for more than 175 days. On the 176th day of the shutdown, the government resumed 2G mobile data and gave access to white-listed websites.⁶¹ Shutdowns in Jammu and Kashmir comprised about 68% of the shutdowns in India, followed by Uttar Pradesh, Rajasthan, and West Bengal. Uttar Pradesh and West Bengal are new hot spots for shutdowns as of 2019.

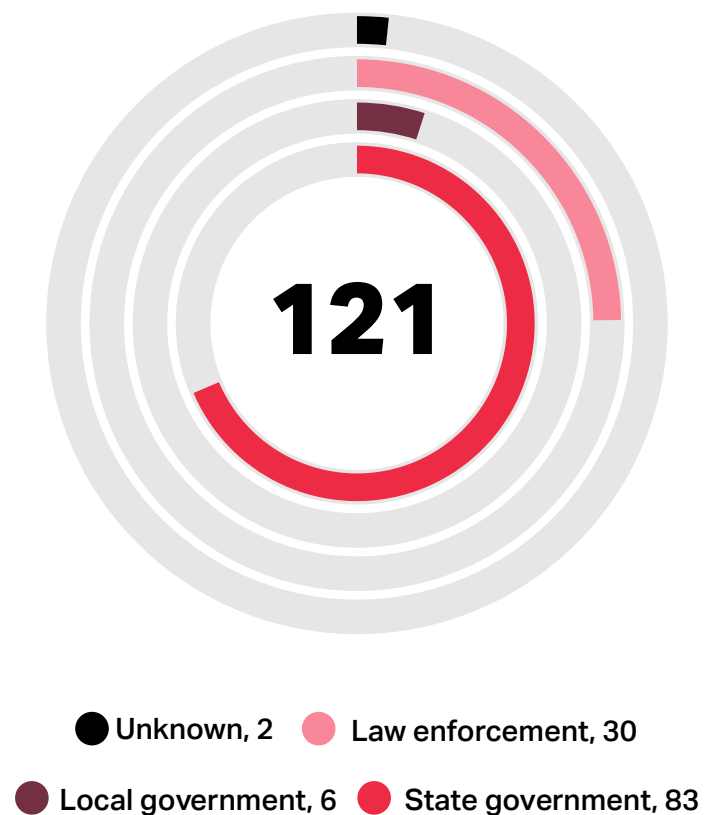
With protests and other challenges to government policies in India, states that did not shut down the internet in 2018 unfortunately resorted to network disruptions in 2019. These include Assam, Bihar, Karnataka, and Tripura.

In contrast to the global trend of countries shutting down the internet during elections, in India, of the total 121 shutdowns observed, only a small proportion were ordered during elections: all were in Kashmir during the 2019 general elections.

In the majority of cases, the orders to shut down the internet in 2019 came from state governments, while in Jammu and Kashmir they were issued by the central government. In India, it is not only the state or central government that orders shutdowns; in some cases, local government or law enforcement agencies order them.

With a few exceptions where the incident was both a throttling and a shutdown, most network disruptions in India are complete shutdowns of mobile telecommunications; that is, authorities cut access entirely and don't resort to slowing down connections. In 2019, authorities cut access to both mobile and fixed-line internet roughly the same number of times that they targeted only mobile internet.

Who ordered internet shutdowns in India ▾



⁶¹ Even though people have access to 2G mobile data, the throttling of mobile data to 2G has effectively continued the blackout in Kashmir as the government is still intentionally denying people meaningful access to the internet.

In India, the most common government rationale for shutting down the internet in 2019 was “precautionary measure” or restoring public order. We have noticed however that shutdowns often take place amidst protests, political instability, military actions by armed forces or paramilitary units, and administrative responses to concerns regarding possible communal violence. It is worth noting that the shutdown orders in Jammu and Kashmir were never made public, with the government refusing to indicate whether the orders were issued under the Telegraph Act’s Network Suspension Rules of 2017, while also trying to assert a broad national security privilege against having to disclose the authority and rationale for the shutdown.

One shutdown that stands out as unique took place in April 2019 at the international border area in Punjab. Authorities ordered a shutdown in the Khemkaran sector in the Indian state of Punjab after a Pakistani drone was spotted flying there in an evident attempt at spying on Indian security forces. The drone was later shot down.

**KASHMIR:
THE WORLD’S SECOND-
LONGEST SHUTDOWN IN 2019**

In 2019, India shut down the internet for 175 days in Jammu and Kashmir. This was the second-longest internet shutdown globally in 2019. It was also among the longest shutdowns we have recorded in India to date.

The shutdown took place after the government introduced legislation to change the political structure in Jammu and Kashmir, following earlier moves which had placed the erstwhile state government under governor’s rule controlled by the central government. The government also banned public gatherings, arrested local leaders, and deployed thousands of troops.^{62 63}

The network restrictions have served to hide a series of egregious reported human rights violations in Kashmir. Numerous news agencies and human rights organizations have published articles with evidence to show that during the blackout in Kashmir, government troops reportedly detained and beat children, some as young as 9 years old.⁶⁴ When authorities implemented the blackout, the government also restricted travel and access to Kashmir. Journalists and the international community have struggled to reach Kashmir, and when they are on the ground, to document and report on the dire situation in the valley. The prolonged shutdown in Kashmir has had another impact on everyday life: as time has passed with Kashmiris disconnected, those eager to check on friends and family saw Kashmiri WhatsApp accounts automatically terminated due to inactivity.⁶⁵

62 Taye, B. (2019, December 19). Urgent: shutdowns in Kashmir, Myanmar, and Bangladesh leave oppressed groups disconnected from the world. Retrieved February 17, 2020, from <https://www.accessnow.org/urgent-shutdowns-in-kashmir-myanmar-and-bangladesh-leave-oppressed-groups-disconnected-from-the-world/>
63 Fareed, R. (2019, August 4). India imposes Kashmir lockdown, puts leaders “under house arrest.” Retrieved February 17, 2020, from <https://www.aljazeera.com/news/2019/08/india-imposes-lockdown-kashmir-puts-leaders-house-arrest-190804174841241.html>
64 Reuters (2019, October 1). Nine-year-old among nearly 150 children briefly held in Indian Kashmir: court probe. Retrieved January 20, 2020, from <https://www.reuters.com/article/us-india-kashmir-children/nine-year-old-among-nearly-150-children-briefly-held-in-indian-kashmir-court-probe-idUSKBN1WG47W>
65 Dixit, P. (2019, December 4). Kashmiris Are Disappearing From WhatsApp. Retrieved February 21, 2020, from <https://www.buzzfeednews.com/article/pranavdixit/hundreds-of-kashmiris-are-disappearing-from-their-whatsapp>

VIII. Rohingya disconnected at home and abroad

Rohingya refugees are one of the most vulnerable communities in the world. For generations in Myanmar, they have been persecuted by the state and denied citizenship and basic human rights. A recent United Nations investigation has called for the Burmese military to be investigated for genocide against the Rohingya and has found that the military has “routinely and systematically employ[ed] rape, gang rape, and other violent and forced sexual acts against women, girls, boys, men, and transgender people.”⁶⁶

These incidents, along with other human rights violations, have forced the Rohingya to flee their home country and seek refuge in neighboring Bangladesh. However, even those who successfully left Myanmar have suffered interference with their rights; many refugee communities were denied internet access in 2019.⁶⁷

MYANMAR: DISCONNECTED AT HOME

In late June 2019, amidst violence and conflict, the Ministry of Transport and Communication ordered all telecom service providers to shut down the internet in nine townships in Rakhine and Chin states in Myanmar. In September, the government partially restored access in five townships, while leaving the rest of the townships completely disconnected from the world.⁶⁸ At the time of publication, the government of Myanmar has reimposed the shutdown in five townships in Chin and Rakhine states.⁶⁹

Civilians living in these conflict zones are unable to reach their loved ones and unable to access information that could be life saving. Civil society, journalists, and humanitarian organizations cannot use the internet to document or publish information about human rights violations or war crimes, and they struggle to provide humanitarian support that often requires the internet to coordinate efforts.

BANGLADESH: DISCONNECTED ABROAD

Those who managed to flee the country and break the shackles of Myanmar’s government have also been denied access to the internet. This time around, it is the Bangladeshi government that is denying them access to the internet, making it illegal for refugees to get access to SIM cards, and restricting mobile phone internet access and 3G and 4G services in Rohingya refugee camps and surrounding areas. A secure and open internet enables refugees to locate and gain access to relief services, correspond with loved ones, and find or share essential and often life-saving information.

Rather than protecting their most vulnerable, these governments are taking actions that put them at even greater risk.⁷⁰

⁶⁶ OHCHR (2019, August 22). UN Fact-Finding Mission on Myanmar Calls for Justice for Victims of Sexual and Gender-based Violence. Retrieved February 21, 2020, from <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24907&LangID=E>

⁶⁷ Teye, B. (2019, December 19). Urgent: shutdowns in Kashmir, Myanmar, and Bangladesh leave oppressed groups disconnected from the world. Retrieved February 17, 2020, from <https://www.accessnow.org/urgent-shutdowns-in-kashmir-myanmar-and-bangladesh-leave-oppressed-groups-disconnected-from-the-world/>

⁶⁸ Reuters (2019, September 1). Myanmar partially lifts internet shutdown in conflict-torn Rakhine, Chin states. Retrieved February 21, 2020, from <https://uk.reuters.com/article/uk-myanmar-rakhine/myanmar-partially-lifts-internet-shutdown-in-conflict-torn-rakhine-chin-states-idUKKCN1VM13L>

⁶⁹ Chau, T. (2020, February 3). Govt doubles down on internet shutdown in western Myanmar. Retrieved February 17, 2020, from <https://www.mmtimes.com/news/govt-doubles-down-internet-shutdown-western-myanmar.html>

⁷⁰ Human Rights Watch (2019, September 7). Bangladesh: Clampdown on Rohingya Refugees. Retrieved February 21, 2020, from <https://www.hrw.org/news/2019/09/07/bangladesh-clampdown-rohingya-refugees>

IX. The #KeptOn coalition in 2019 and 2020

The #KeptOn coalition and community has been working around the clock to prevent, identify, verify, and document incidents of shutdowns around the world. Our community has grown: we started the year with 170 coalition members and ended with 210. Working together, we have verified and documented shutdown cases, collected stories from victims to amplify their voices, facilitated cross-sector efforts to build a problem-solving framework, and litigated against shutdowns. We have stretched outside of our community to engage additional actors, governments, platform service providers, and members of the internet access and measurement community.

Engaging with governments and international bodies

As more countries have engaged in shutting down the internet in 2019, some have also been vocal about the danger of such interferences. For example, the U.S. Department of State expressed concern at internet restrictions in Jammu and Kashmir.⁷¹ The #KeptOn coalition encourages states to use their good offices to denounce internet shutdowns and their disproportionate impact on people's lives. The U.S. House of Representatives recently passed a resolution that denounced internet shutdowns. House Resolution 358 introduced by Congresswoman Karen Bass "call[s] on the

government of Cameroon and armed groups to respect the human rights of all Cameroonian citizens and to end all violence."⁷² The resolution explicitly states that the Cameroonian government's decision to shut down the internet undermines freedom of expression.

Back in 2017, we had saluted the commitment by 30 governments of the Freedom Online Coalition (FOC) to fight against network disruptions.⁷³ Since then, we have continued to engage with FOC governments and others and even had the opportunity to share background information to inform and guide their diplomatic community's response to internet shutdowns. Some of these governments and members of the diplomatic corps have directly reached out to the #KeptOn coalition to report incidents of shutdowns and to seek information about impeding shutdowns.

International institutions and Special Rapporteurs have also played a role in denouncing internet shutdowns and their harmful impact on people's human rights. In July 2019, U.N. experts denounced measures taken by the authorities to shut down the internet in Sudan, saying it stifles free expression and association.⁷⁴ Such public statements are instrumental to assert the rights of affected communities, and to counter the growing assumption that internet shutdowns can be legitimate measures, especially in times of unrest or conflict.

⁷¹ The Bureau of South and Central Asian Affairs (SCA) (2020, January 11). "Closely following @USAmblIndia & other foreign diplomats' recent trip to Jammu & Kashmir. Important step. We remain concerned by detention of political leaders and residents, and internet restrictions. We look forward to a return to normalcy. AGW." Retrieved February 20, 2020, from https://twitter.com/State_SCA/status/1216050174713368577

⁷² U.S. House of Representatives (2019, June 26). Text - H.Res.358 - 116th Congress (2019-2020): Calling on the Government of Cameroon and armed groups to respect the human rights of all Cameroonian citizens, to end all violence, and to pursue a broad-based dialogue without preconditions to resolve the conflict in the Northwest and Southwest regions. Retrieved February 21, 2020, from <https://www.congress.gov/bill/116th-congress/house-resolution/358/>

⁷³ Access Now (2017, April 6). 30 governments step it up to denounce internet shutdowns at RightsCon Brussels. Retrieved February 20, 2020, from <https://www.accessnow.org/30-governments-step-denounce-internet-shutdowns-rightscon-brussels/>

⁷⁴ OHCHR (2019, July 8). Sudan: UN experts denounce Internet shutdown, call for immediate restoration. Retrieved February 20, 2020, from <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24803&LangID=E>

Grassroots grants help #KeepItOn

As more and more people around the world are affected by prolonged and targeted shutdowns, it is imperative that we as the #KeepItOn community support and fund grassroots efforts that are organizing to deter and circumvent shutdowns. Access Now's Grants program, which provides grants to grassroots and frontline organizations fighting for human rights in the digital age, aims to identify and support communities that are most affected by shutdowns.

In 2019, we supported the Media Foundation for West Africa (MFWA) in organizing a regional convening to discuss the issue of elections and internet shutdowns in the region. This convening brought together government officials, election authorities, and other relevant actors to address the issue, a threat in the region given the election-related shutdown in Benin and fear of shutdowns during Senegal's and Nigeria's elections.

Internet shutdowns do not happen on a normal day. They often take place during periods of political instability. This makes it harder for grassroots groups to organize, whether to fight shutdowns or address any other human rights violations. In 2019 we funded private convenings for people in North Africa and the Red Sea region. One meeting took place outside of a country in a state of crisis to enable activists and human rights defenders to think and speak freely. This support gave these at-risk activists a safer space to develop new tactics to circumvent or prevent future shutdowns, as well as an opportunity to build connections with the regional and global digital rights communities, deepening the technical and strategic support and solidarity they need to carry the fight forward.

Myanmar was the site of prolonged shutdowns in 2019, and we provided funding for organizations like Free Expression Myanmar (FEM) and Athan with the aim of strengthening their advocacy and policy work on freedom of expression and access to information. This is especially important as armed conflict and gross human rights violations have taken place in the lead-up to an election in 2020.⁷⁵

Sometimes, members of the #KeepItOn community simply need support to get their work in front of the right audience. We were proud to fund the effort of our partners in Cameroon to bring their documentary on shutdowns, *Blacked Out*, to RightsCon, Access Now's annual summit on human rights in the digital age, which took place in 2019 in Tunisia.⁷⁶

Challenges and opportunities

It is befitting to end the 2019 #KeepItOn report with some of the challenges we have faced, as it was a difficult year for those of us fighting to end shutdowns across the globe. On a more positive note, we also see opportunities opening to further strengthen our work.

The epidemic of shutdowns continues to grow. In 2019, we saw an increase in shutdowns globally, with a trend toward more targeted and prolonged shutdowns. This compounds the harm to extremely vulnerable populations. In countries that are imposing these shutdowns, civil society is increasingly at risk, and so too are the causes they are fighting for. For our coalition, this raises critically important questions about safety and security.

In 2019, we engaged in difficult conversations about what it means to do this work, how to

⁷⁵ Chau, T. (2020, February 3). Govt doubles down on internet shutdown in western Myanmar. Retrieved February 17, 2020, from <https://www.mmmtimes.com/news/govt-doubles-down-internet-shutdown-western-myanmar.html>

⁷⁶ Blacked Out Pictures (2019, June 1). RightsCon Tunis 2019: BLACKED OUT: A documentary about the longest internet shutdown ever recorded. Retrieved February 21, 2020, from <https://rightscon2019.sched.com/event/PvrS/blacked-out-a-documentary-about-the-longest-internet-shutdown-ever-recorded>

put ethics and the security of users at risk first, and whether our means suit our ends. We have pushed members of the technical community that verify, measure, and track internet connectivity to develop clear and transparent methodology to show how they detect and document internet outages. We have also asked those offering measurement tools to give users as much information as possible about risks associated with these tools and the information they collect, and to be transparent about how they use or share the collected data.

We see a new opportunity to engage the courts and judiciaries at national and international levels in the fight against shutdowns. Jurists understand that human rights apply online, and more lawyers are challenging governments and telcos for blocking access. While lawsuits aren't appropriate in every situation, they can be effective in many countries, and Access Now's Digital Rights Litigators Network stands ready to support potential litigants. In the fight against internet shutdowns, we also see our community becoming more resilient and supporting efforts to circumvent internet disruptions, challenge shutdowns through legal avenues, and document human rights violations even during an internet shutdown. For example, #KeptItOn member WITNESS released useful tips and approaches to capturing and preserving video documentation during internet shutdowns.⁷⁷ These kinds of resources, together with lawsuits, are possible thanks to the relentless efforts of the growing movement against internet shutdowns around the world, which includes the documentation and analysis of incidents, as well as the collection of testimonies from people who have experienced shutdowns.

As we look ahead to 2020, we hope to foster the development of a community standard for the use of measurement technology that makes the safety and security of users at risk the top priority. We plan to continue supporting legal challenges to shutdowns and pushing for laws and policies that disallow shutdowns, an inherently blunt and disproportionate interference with the rights to free expression and access to information. We will strive to document every shutdown that governments order and assist internet service providers around the world in increasing transparency and pushing back against shutdown orders. We will also keep funding grassroots organizations to support each of these efforts. We hope you join us in this fight.

⁷⁷ WITN Ng, Y. (2020, January 31). Documenting During Internet Shutdowns. A blog series with practical tips. Retrieved February 20, 2020, from <https://blog.witness.org/2020/02/documenting-during-internet-shutdowns/>

CONTACT

For questions and more information, please visit
<https://www.accessnow.org/keepiton/>

Or reach out to
Berhan Taye at berhan@accessnow.org
Felicia Anthonio at felicia@accessnow.org

TARGETED, CUT OFF, AND LEFT IN THE DARK

The #KeepItOn report on internet
shutdowns in 2019

#KeepItOn 

