Internet Shutdowns in 2016

Japreet Grewal
The Centre for Internet and Society, India
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. There is no consolidated research on internet shutdowns worldwide and government policies relating to this phenomenon. Access, however, has been tracking instances of internet shutdowns here. According to this tracker, there were 56 internet shutdowns worldwide in 2016.

In this report, we have identified countries where shutdowns took place more than once in the past one year. We were able to identify these countries from the tracker that is being operated by Access. We have looked at the internet shutdown practices and government policies on shutdowns in these countries. The countries include Brazil, Egypt, Ethiopia, Gambia, India, Iraq, Pakistan, Syria, Turkey and Uganda.

We have greatly relied on media coverage of internet shutdowns in the aforementioned countries and reports by various organisations including Freedom House, Amnesty International, Human Rights Watch, Article 19, Access, Electronic Frontier Foundation, Brookings Institution, Annenberg School of Communication, OSCE, Centre for Communication Governance, OONI and Dyn documenting and/or analysing internet censorship in these countries.

While documenting internet shutdown practices in the countries identified above, we have looked at the geographical coverage of a shutdown i.e. whether it was carried out nationwide or in specific regions and type of internet services that were restricted i.e. whether access was restricted to the whole internet, mobile internet services or specific messaging services and/or applications. In this regard, we have referred to a report published by the Brookings Institution, Internet shutdowns cost countries $2.4 billion last year that has analysed the economic impact of internet shutdowns. In this report, the author has identified six categories of disruptions: national internet, subnational internet, national mobile internet, subnational mobile internet, national app/service, and subnational app/service. I have used this classification to understand and document internet shutdown practices in the aforementioned countries.

Please see the information documented in the table below.

<table>
<thead>
<tr>
<th>Country</th>
<th>Internet</th>
<th>Mobile Internet</th>
<th>Service/Application</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>National</td>
<td>Subnational</td>
<td>National</td>
<td>Subnational</td>
</tr>
<tr>
<td>INDIA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Rohtak, Haryana</td>
<td>Jammu &amp; Kashmir</td>
<td>Gujarat</td>
<td>Bokaro, Jharkhand</td>
</tr>
<tr>
<td>Country</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>-----------</td>
<td>----</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Egypt</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ethiopia</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Gambia</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iraq</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Syria</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Turkey</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Uganda</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

In the first incident, Facebook and Twitter became inaccessible. In the second incident, access to Instagram, Facebook, Twitter, YouTube and Vimeo was blocked.
While documenting government policies on internet shutdowns, we looked at the reasons given by the governments for imposing internet shutdowns, the legislation pursuant to which the internet shutdowns could be carried out or were carried out, the authority that issued orders for internet shutdowns and legal challenges questioning the validity of internet shutdowns, if any, in these countries.

**Ethiopia**

The Ethiopian government carried out internet shutdowns in the country to suppress protests against the government censorship on some occasions and to prevent students from cheating during exams on others. In August 2016, the Ethiopian government shut down internet services for two days in response to the anti-government protests. Reports also suggest that certain services were down for almost a month.

**Law**

Under the Ethiopian Constitution, every individual has the freedom of expression. Article 26 that grants the freedom of expression also states that freedom of expression and information cannot be limited on account of the content or effect of the point of view expressed. This freedom however can be limited in order to protect the well-being of the youth, and the honour and reputation of individuals. Any propaganda for war as well as the public expression of opinion intended to injure human dignity is prohibited by law. This freedom may be suspended during the state of emergency.

Under Article 93 of the Ethiopian Constitution, the Ethiopian government is empowered to declare a state of emergency in case of an external invasion, breakdown of law and order in the country which endangers the constitutional order and which cannot be controlled by the regular law enforcement agencies and personnel, a natural disaster, or an epidemic. A state of emergency can also be declared by state executives during natural disaster or an epidemic. According to a report authored by Human Rights Watch, in the state of emergency, the emergency declaration allows the Command Post to issue a directive to stop or suspend any mass media and communications throughout the country.

There is no legislation in Ethiopia that allows an internet shutdown. According to a report written by OONI and Amnesty International last year, the telecommunications, cybercrimes, security, and intelligence laws do not have provisions that govern content control and access to internet in the country. The laws that established the security agencies in Ethiopia namely, Information Network Security Agency and the National Intelligence and Security Service authorize neither of the institutions to restrict access to internet and social media, censor websites for any reason. The Telecom Fraud Offences Proclamation does not authorize any of the Government agencies to control and restrict access to internet, websites, or social media application in the country.

EthioTelecom has unilateral control over the telecommunications infrastructure in the country. The Ethiopian government’s monopolistic control over EthioTelecom has empowered it to control the telecommunication infrastructure. It enables the government to restrict information flows and access to internet and mobile phone services. There has been no legal challenge yet to the shutdowns.

**Gambia**

In Gambia, internet shutdowns have been carried out to suppress protests against the incumbent government. Internet was also shut down on the eve of elections. Media reports claimed that this was done to stifle opposition.

**Law**

The Constitution of Gambia provides freedom of expression to every individual, which may be limited in the interests of the sovereignty and integrity of the nation, national security, public order, decency or morality, or in relation to contempt of court. Under Article 34 of the Gambian Constitution, the President can declare a state of public emergency in whole or part of the country and the authority can derogate from the constitutional sanction of freedom of expression as long as it is reasonably justifiable in the circumstances arising or existing during a period of public emergency for
the purpose of dealing with the situation. According to the Freedom House report, former president Jammeh is known for his utter disregard for constitutional rights, stating publicly in March 2011 that he would not compromise or sacrifice the peace, security, stability, dignity, and the well-being of Gambians for the sake of freedom of expression.

The Public Utilities and Regulatory Authority (PURA) has been set up under the Public Utilities and Regulatory Authority Act, 2001 has the responsibility for the regulation of information and communications services, information and communications networks, associated facilities and associated services. It is the national regulator of telecommunication services in the country.

There is limited information available about the legal provisions under which internet services were disrupted in 2016. The Information and Communication Act, 2009 and the Criminal Code 1933 does not make it clear if the PURA has the legislative power in issuing directives for disruption of internet services. However, old Freedom House Reports on Gambia (specifically Freedom on the Net Report 2015) have stated that the service providers claim that the disruptions happen because of technical difficulties. In fact, news reports state that information about the shutdowns in 2016 came from Gambia Telecommunications Company Limited (Gamtel) insiders. Gamtel is a state-owned telecom company and this company owns the fiber-optic cable that runs across the country and controls the country’s connection to the international internet. According to the Freedom House report, the government denies any involvement in the blocking of communication services like Whatsapp or Viber; however, there have been speculations that the state control over the country’s dominant telecommunications provider, Gamtel, gives the authorities the ability to restrict access to internet content.

The government of Yahya Jammeh has been thrown out of power. There has been no challenge to these internet shutdowns yet.

Uganda

During the election in February, Ugandan authorities blocked all access to social media for three days, citing security concerns. Social media was also blocked in May 2016 during Ugandan president Yoweri Museveni swearing in ceremony. The telecom regulator of Uganda have issued orders for internet shutdown to disrupt security threats, curb any kind of misinformation and illegal election campaigning.

Law

The Ugandan Constitution protects freedom of speech of every individual under Article 29. However, this freedom can be restricted in public interest provided that such limitation cannot be beyond what is acceptable and demonstrably justifiable in a free and democratic society, or what is provided in this constitution. This freedom can also be restricted in a state of emergency under Article 46 of the Ugandan Constitution provided such restriction is reasonably justifiable to the requirements during an emergency. A state of emergency can be declared under Article 110 of the Ugandan Constitution in case of war or external aggression, internal insurgency or natural disaster, or in circumstances that make it necessary to take measures which are required for securing the public safety, the defence of Uganda and the maintenance of public order and supplies and services essential to the life of the community.

The Uganda Communications Commission (UCC) is a government regulatory body that was set up under the Uganda Communications Act, 1997 and is responsible for licensing, regulation and development of the communications infrastructure in Uganda. UCC has informed the media that the disruption of internet services has been done under Section 5 (1) (b) and (Section 5 (x)), of the Uganda Communications Act, 2013. According to the Freedom House Report, UCC has claimed that these provisions allow the regulatory body to “monitor, inspect, license, supervise, control and regulate communications services” and to monitor and enforce compliance relating to content.

Following the internet shutdowns, a non-governmental organisation, Legal Brains Trust, has taken the government to court over this decision on the ground that this move was irrational and that property, livelihood and consumer rights connected with mobile money transactions had been disproportionately interfered with by the state.
Syria

Media reports claim that the internet shutdowns have been carried out in Syria to prevent the dissemination of information before and during offensive military operations. However, according to the official communication by the telecom regulator, the internet blackout in the country in October 2016 was due to cable repairs, which reportedly resulted in a blackout of 60% of the internet. The telecom regulator has also shut the internet in Syria to prevent cheating in national high school exams. These shutdowns would last for about four hours a day and continue for almost ten days. In another instance of internet shutdown, it has been claimed that this disruption was incidental to regular power cuts in the country.

Law

The Syrian Constitution under Article 42, guarantees freedom of expression to every individual and does not shed much light on the restrictions, if any that could be placed on this freedom. A state of emergency can be declared by the President as mentioned in Article 103 of the Constitution however the grounds on which emergency can be declared are absent.

The Syrian Telecommunications Establishment (STE) serves as both an internet service provider (ISP) and the telecommunications regulator in areas controlled by the Syrian government. STE is state owned enterprise and according to the report by Freedom House, this provides the Government with tight control over internet infrastructure thus allowing the Government to issue internet shutdown orders via STE. Based on media reports and research done by various international organisations, there is not much clarity about the legislation under which the orders to shut down access to internet and/or social media services are passed by the government/STE. According to a source, a cybercrime law that was passed in February 2012 provides a legal basis for website filtering and blocking. However, the Government has often claimed that internet shutdowns have been caused due to technical difficulties.

There have been no legal challenges against the censorship that is being carried out in Syria. According to the Freedom House report, the judiciary lacks independence and its decisions are often arbitrary.

Iraq

Internet shutdowns have been carried out in Iraq to suppress protests and prevent cheating in exams. In an attempt to prevent cheating in exams, Iraq saw three separate three hour disruptions to internet service in May 2016. The blockade, which affected fixed-line and mobile broadband, was mandated by the Iraqi ministry of communication. The Iraqi government also shut down internet reportedly for around four hours in response to anti-government protests in the capital of Baghdad.

Law

Article 36 of the constitution of Iraq guarantees freedoms of expression and the media but this freedom may be limited on the ground of public order or morality.

The Ministry of Communications gives the order to block access to the fibre network in the country from ISPs. The government essentially owns the internet infrastructure (fibre optic cable connecting major cities in Iraq) and this is operated by the Iraqi Telecommunications and Post Company (ITPC).

Egypt

Internet shutdowns are frequent in heavily militarised areas of North Sinai and are claimed to be carried out to deter communications between insurgent groups in the area. In September 2016, one such shutdown lasted for 8 hours before the services were restored. Signal, a messaging app, was reportedly shut down for a week in December 2016. Media reports claim it was to stifle political dissent.
**Law**

Article 65 of the 2014 Egyptian Constitution guarantees freedom of thought and opinion and Article 70 establishes freedom of press.

Article 67 of the Egypt Telecom Regulation Act, 2003 confers wide powers on the National Telecommunication Regulatory Authority (NTRA) to regulate telecommunication services. This law empowers NTRA to regulate telecommunication services with the objectives of “protecting national security and the State’s top interests.” Further, Article 67 provides competent authorities the power to completely seize control of any or all telecommunication services in the case of natural or environmental disaster, or during declared periods of general mobilization or any other case concerning national security. The provision does not clarify who the “competent authorities” are. This provision was used by state authorities as a legal basis to shut down the mobile phone network and the internet completely for five days, in response to protests in January 2011 claiming threat to national security.

This was challenged by the human rights activists in Egypt’s highest administrative law court, Council of State. The judges held that protestors did not threaten national security, only the security of a regime which (they argued) had lost its legitimacy. They further stated that shutdown of communications and Internet services exposed the security and the lives of Egyptians to unnecessary danger and concluded this exercise violated public freedoms and constitutional protections of the right to communicate, freedom of expression, privacy, press freedom and freedom of information. The judges also held that definition of national security had to be expanded to include social justice, economic development, human dignity, and freedom. The judgement also commented authoritatively on the powers of the NTRA and its role in the operation of the shutdown; in particular the judges gave a detailed account of the NTRA’s role in every stage of the internet shutdown, showing that the NTRA was the representative of the ministry of telecommunications and information technology in the operations room which managed the shutdown – alongside representatives from the armed forces and the security services.

Egypt has also passed a new anti-terrorism bill that allows the State to monitor social media and block sites.

**Turkey**

Internet shutdown in Turkey is usually carried out in order to suppress media coverage or prevent negative coverage of political incidents and avoid panic and public disorder following a political crisis (terrorist attacks/military coup). Turkey declared a state of emergency in July, 2016 following an unsuccessful military coup. The emergency is still in effect. In this period, the Turkish Government passed fifteen decree laws some of which have been aimed at digital surveillance of users and the shutting down of internet service at times of so-called security operations. The TIB was closed down by the Government in August 2016 via a decree and the powers of TIB were transferred to ICTA. The Government has cut access to internet via landline and mobile in certain regions following a political crisis to suppress protests and also blocked access to Twitter, Facebook, YouTube, as well as WhatsApp throughout the country on the grounds of security. The Government has also ordered Turkish ISPs to block popular VPN services and Tor Network.

**Law**

Article 26 of the Turkish Constitution provides that every individual has the freedom of expression may be restricted for the purposes of protecting national security, public order and public safety, the basic characteristics of the Republic and safeguarding the indivisible integrity of the State with its territory and nation, preventing crime, punishing offenders, withholding information duly classified as a state secret, protecting the reputation and rights and private and family life of others, or protecting professional secrets as prescribed by law, or ensuring the proper functioning of the judiciary.

Article 22 of the Turkish Constitution provides the right to freedom of communication to every individual which can be restricted on the grounds of national security, public order, prevention of crime commitment, protection of public health and public morals, or protection of the rights and
freedoms of others only upon a decision duly passed by a judge or by a written order of an agency authorised by law in cases where delay is prejudicial. The decision of the authorised agency shall be submitted for the approval before a judge having jurisdiction within 24 hours. The judge shall announce his decision within 48 hours from the time of seizure; otherwise, seizure shall automatically be lifted.

Article 15 of the Turkish Constitution states that fundamental rights and freedoms guaranteed under the Constitution can be partially or fully suspended in times of war, mobilization, martial law, or state of emergency, provided that obligations under international law are not violated. Article 120 of the Turkish Constitution empowers the government to declare a state of emergency if there are serious indications of widespread acts of violence that are aimed at destroying the free democratic order established by the Constitution or of fundamental rights and freedoms, or serious deterioration of public order because of acts of violence. The emergency cannot be declared for more than 6 months.

Under the Regulation on Authorisation of Electronics Communication Sector, the Information and Communication Technologies Authority (BTK) is responsible to grant approval for delivery of telecommunication services. An amendment was made in June 2016 under which BTK (Information and Communication Technologies authority) can now “partially or entirely” suspend internet access due to war / national security and is no longer required to seek ministerial oversight in taking such actions. The same amendment also allows the authority to take over ISPs and control them directly.

The Regulation of Publication on the Internet and the Suppression of Crimes Committed by means of such Publication, 2007 (Law no. 5651) regulates internet and online service providers and determines conditions for blocking access to these websites. Blocking orders can be issued under this law by courts, public prosecutors as a precautionary injunction, or the Telecommunications Communication Presidency (TIB). This law was amended in 2014 to expand the TIB’s authority to block websites and their content without court permission. The Turkish Constitutional Court declared unconstitutional the amendments to this law which permitted the TIB to block any website without prior court orders for reasons of national security, the restoration of public order, or to prevent a crime from being committed.

Despite the rulings of Turkey’s top court, the government had made it clear that it would keep trying to exert greater control over the Internet with another law.

Pakistan

In Pakistan last year, shutdowns were carried out primarily on grounds of national security in anticipation of terrorist attacks and/or on religious or national holidays, protests and marches. Shutdowns usually block mobile services, such as voice, SMS and mobile Internet.

Law

Article 19 of the Constitution of Pakistan establishes freedom of speech which can be restricted by law in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, commission or incitement to an offence. The freedom guaranteed under Article 19 stands suspended during the state of emergency under Article 233. However, Article 232 of the Pakistan Constitution states that a state of emergency can be declared by the President only on grounds of threat to the security of the nation by war or external aggression, or by internal disturbance which is beyond the control of a provincial government.

Suspension of internet services is carried out under the Pakistan Telecommunications (Re-organisation) Act by the Pakistan Telecommunication Authority established by this legislation. The internet shutdowns are justified under Article 54(2) and 54(3) of this legislation on grounds of national security. According to the Article 19 report, a number of law enforcement agencies are authorised to request network shutdowns to the PTA which then verifies these requests and directs service providers to carry out a shutdown in a specific region. The identity of these agencies remains confidential and not public knowledge. Article 54 (2) states that during a state of emergency, the federal government “shall have preference and priority in the telecommunication system over any
licensee”. Section 54(3) empowers the federal government to suspend or modify existing telecom licences or cause suspension of operation, functions or services of any licensee during an emergency.

A writ petition was filed by a telecommunication company in Pakistan Telenor in the Sindh High Court, contesting the use of Section 54(3) for invoking network shutdowns, since these powers can only be invoked if a state of emergency has been declared in the country. Telenor Pakistan believes that in the absence of a state of emergency, the provision does not apply and therefore network shutdowns are orders without any legal basis. Several similar petitions were also filed to challenge network shutdowns for the reasons that these shutdowns caused disruption in their personal and professional lives and were a threat to their security and wellbeing. The matter is still pending in the court.

Brazil

According to the Freedom House Report, the government does not impose control over telecommunications infrastructure. There have been no reported instances of the government cutting off internet connectivity during protests or social unrest. However, Brazilian Courts have suspended instant messaging services such as Whatsapp in the country due to the failure of the company in cooperating in criminal investigations. Failure to hand over data requested by courts has been held the reason for repeated nationwide suspensions. In May 2016, a lower court ordered a nationwide shutdown of Whatsapp for 72 hours. On similar grounds, Whatsapp was shut down for a few hours in July before the Supreme Court overturned the order directing this shutdown.

Law

Article 5 of the Federal Constitution of Brazil guarantees freedom of expression. Further, Article 3 of the Marco Civil de Internet (Brazil’s Internet Constitution) guarantees freedom of expression, communication and expression of thoughts, under the terms of the Federal Constitution of Brazil.

Courts, however have issued orders for suspension of messaging services like Whatsapp across the country. The Brazilian Supreme Court ultimately overturned an indefinite suspension of Whatsapp and held that “the suspension of the service apparently violates the basic principle of freedom of expression and communication, enshrined in the Constitution, as well as prevailing legislation on the matter.” The Court held that the ban was “disproportionate.”

India

Internet shutdowns are increasingly becoming common in India. According to an assessment done by Software Freedom Law Centre in India, they are usually instituted in response to conflict situations i.e. to prevent rumor-driven escalations of civil unrest, but they are also instituted at times for reasons far more trivial, such as to prevent cheating during examinations. Until last month, 63 shutdowns have been reported across 12 Indian States, with the State of Jammu and Kashmir topping the list at 27 shutdowns instituted since 2012. These internet shutdowns are usually carried out in specific regions and most commonly on mobile internet.

Law

The government usually uses Section 144 of the Code of Criminal Procedure as a legal basis to shut down internet services. Section 144 permits the state or the central government to issue an order to “prevent... obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, of an affray”. It requires a written order from a magistrate. Section 144 can only be used as a last resort only when ‘a lesser alternative would be inadequate’.

Another legal basis for disruption of internet services may be Section 5 (2) of the Telegraph Act 1885. This provision has been expanded over the years to give the central or state government the power to stop transmission of messages in the interest of public order or for preventing incitement to the commission of an offence. These restrictions fall within the contours of Article 19 (2) of the Indian Constitution. Reference can also be made to the Licence Agreement for Unified Licence between
a telecommunication company and the Central Government (more specifically, the Department of Telecommunications). Clause 39.15 under Chapter VI (Security Conditions) states this, 

“The Government through appropriate notification may debar usage of mobile terminals in certain areas in the country. The LICENSEE shall deny Service in areas specified by designated authority immediately and in any case within six hours on request.”

An argument has also been made in favour of using Section 69 A of the Information Technology Act, 2000 as a legal basis for issuing an order for internet shutdown. This provision gives powers to the Central Government to block access “by public any information generated, transmitted, received, stored or hosted in any computer resource.” This provision has been invoked to disrupt access to information on the internet but has not been used to suspend access to internet via landline and mobile. Further, under this provision a direction by Central Government is required to ban internet communication.

A case was filed in the High Court of Gujarat challenging the internet ban in th estate of Gujarat. It was argued that the power to suspend internet was under Section 69A of the Information Technology Act, 2000 hence the government could not resort to a much broader provision like Section 144 of the Code of Criminal Procedure. The court upheld the internet ban. The court held that there was no necessity to block all social media sites and infact, restricting speech only by a mobile internet ban was reasonable as the citizens still had access to the internet through broadband and wifi. The petitioner filed a Special Leave Petition in the Supreme Court; however, the Supreme Court upheld the decision of the Gujarat High court and dismissed the SLP.

**Conclusion**

We have made some significant observations in our survey of government practices and policies on internet shutdowns.

At present, there is no set of principles or global norms that dictate the circumstances under which the governments are authorised to disrupt access to internet services, determine the mode, extent and duration of such disruption and a procedure that must be followed to issue an order to shut down the internet.

There appears to be no clarity about the legal basis in the countries, that we have surveyed, upon which the governments in these countries can issue orders to shut down the internet. Governments worldwide, have disrupted access to internet services in varying circumstances (note, elections, emergency, protests have been most common circumstances) justifying these actions in the interest of public order or national security. While there is an established jurisprudence on public order and national security, their application has been inconsistent with the principles of necessity and proportionality.

We have observed that the legal basis for the power to issue an order for internet shutdown has emerged from the telecommunication laws, emergency laws or cybercrime laws. The language of these legislations is usually overbroad and vague. These laws do not provide clarity about specific circumstances in which an order for internet shutdown can be issued, mode of internet shutdown, the geographical extent, duration. In certain countries there is no legal basis for the government or the regulator to disrupt access to internet services and this is done by virtue of the government’s control over the telecom infrastructure in the country. In fact, in several countries that we have surveyed, the regulatory authority for telecommunications is not an autonomous body and is under the control of the government.

It is notable that the constitutional law in most of these countries has established the legal standards for protection of human rights including the freedom of expression and the circumstances under which it can be restricted. In several countries, internet shutdowns have been challenged in the courts however, the judicial response to these incidents has been slow, sluggish and not protective of free speech in most of the countries that we surveyed barring a few countries like Turkey and Brazil.

Internet shutdown is becoming a popular instrument of repression among the governments (whether these are autocracies or democracies) worldwide. The existing legal frameworks have increasingly failed to regulate the government’s powers and are being used to merely justify these practices. There is an urgent need to set global standards for internet shutdown practices to address this growing problem of internet shutdowns.
ENDNOTES

[1] Japreet Grewal, Centre for Internet & Society
[2] This definition has been formulated by several technical experts at RightsCon in 2016. Access Now refers to this definition for th purpose of its campaign, KeepItOn.
[7] To Beat Exam Cheats, Gujarat to Block Mobile Internet Today. The Times of India, February 2016; Mobile Internet Services Cut off in Gujarat Districts & Bokaro, Jharkhand, MediaNama, April 2016
[8] Internet Services Blocked in Bokaro after Communal Tension. The Times of India, April 2016; Mobile Internet Services Cut off in Gujarat Districts & Bokaro, Jharkhand, MediaNama, April 2016
Twitter, WhatsApp Down in Ethiopia Oromia Area After Unrest, Bloomberg; Ethiopia: Reform Only Feasible Way out of Mounting Crisis; Ethiopia Offline, Amnesty International & OONI; Ethiopia declares state of emergency after months of protests, CNN; Ethiopian authorities shut down mobile internet and major social media sites, Global Voices (blog)


Syria’s state mobile provider said its internet service had been “partially cut due to part of the network unexpectedly malfunctioning”, Middle East Eye, March 2016, available at http://www.middleeasteye.net/news/unexpected-power-cut-leaves-whole-syria-without-electricity-1940175552


Social media blocked in Turkey, August 25, 2016 [31]


Twitter, WhatsApp Down in Ethiopia Oromia Area After Unrest, Bloomberg


Freedom on the Net 2015- Gambia 2015, Freedom House


UCC Act, 5(1)(b) to monitor, inspect, licence, supervise, control and regulate communications services;

UCC Act, 5(1)(x) to set standards, monitor and enforce compliance relating to content; and


Syrian Telecom Announces 10-Day Internet Blackout, The Daily Beast, October 2016, available at http://www.thedailybeast.com/cheats/2016/10/18/syrian-telecom-announces-10-day-internet-blackout.html; Syria Announces A 10-Day Internet Blackout For ‘Submarine Cable Repairs’ and Russia May be to Blame,

[53] Syria's mysterious internet blackout solved: Government switches off entire web to stop exam cheats, International Business Times; Syria goes to extremes to foil cheaters, Dyn

[54] Syria's state mobile provider said its internet service had been "partially cut due to part of the network unexpectedly malfunctioning", Middle East Eye


[57] https://internetlegislationatlas.org/data/summaries/syria.pdf

[58] Freedom on the Net 2016 - Syria, Freedom House

[59] Iraq shuts down the internet to stop pupils cheating in exams, The Guardian

[60] Iraq Shuts Down Internet In Response To Baghdad Protests, Silicon


[62] How Iraq Turned off the Internet, Wired UK


[64] No Signal: Egypt blocks the encrypted messaging app as it continues its cyber crackdown, TechCrunch, December 26, 2016 https://techcrunch.com/2016/12/26/1431709/


[68] Internet shutdown in Turkey's Southeast, Turkey Blocks; New internet shutdown in Turkey's Southeast: 8% of country now offline amidst Diyarbakir unrest, Turkey Blocks, October 2016, available at https://turkeyblocks.org/2016/10/27/new-internet-shutdown-turkey-southeast-offline-diyarbakir-unrest/; Facebook, Twitter, YouTube and WhatsApp shutdown in Turkey, Turkey Blocks


[70] Turkey Blocks Facebook, Twitter, and YouTube Amid Military Coup, Fortune


[73] Decree Law 671 amends the Law of Digital Communications and allows the BTK to overtake any privately-held digital communications company including cable or cellular network providers to “[maintain] national security and public order; prevent crime; protect public health and public morals; or protect the rights and freedoms [of citizens].”; Turkey's Internet Policy after a Coup Attempt, Annenberg School of


[75] New internet shutdown in Turkey's Southeast: 8% of country now offline amidst Diyarbakir unrest, Turkey Blocks


[80] Turkish government's social media throttling in Turkey points to wartime censorship efforts, The Daily Dot; Article 10, Electronic Communications Authorization Related To Sector Changes In The Regulation. - - - The heading of Article 21 of the same Regulation has been amended as follows and the following paragraph has been added to the same article. Preventing service delivery and suspending the business”

“(2) Authority; In the event of war, general mobilization and the like, public safety and national defense, it may suspend all or part of the business activities of the operator for a limited or unlimited period and may operate the direct network. In this case, the deadline is added at the end of the authorization period. “; http://www.resmigazete.gov.tr/eskiler/2016/06/20160611-1.htm

[81] Under Article 8(1) access to websites are subject to blocking if there is sufficient suspicion that certain crimes are being committed on a particular website. The eight specific crimes that are included in Article 8 are: encouragement of and incitement to suicide, sexual exploitation and abuse of children, facilitation of the use of drugs, provision of substances dangerous to health, obscenity, gambling, and crimes committed against Atatürk


[89] Pakistan: Government must stop ‘kill switch’ tactics, Article 19


[93] Rafael Barifouse, Fernando Duarte, Guilherme Barrucho, “Por que o bloqueio do WhatsApp não vingou – e como isso afetará a briga entre empresas de internet e Justiça” [Why the blocking of WhatsApp did not succeed – and how this will affect the fight between internet companies and Justice], BBC Brasil, December 2015, available at http://bbc.in/1mbcOmp.


[96] WhatsApp Ordered Blocked Again in Brazil Over Data Dispute, Bloomberg


[100] Section 144 of CrPC available at https://indiankanoon.org/doc/930621/


[102] Ramila Maidan Incident v. Home Secretary, Union of India & Ors WRIT PETITION (CRL.) NO. 122 OF 2011

[103] Section 5 (2) of the Indian Telegraph Act, 1885 available at https://indiankanoon.org/doc/1445510/


