Internet shutdown and social media platform blocking in Indo-Pacific

Open Net Association

I. Introduction

The extremely distributed architecture of the Internet has a civilizational significance of having given all powerless individuals an agency in mass communication previously available only to newspapers and broadcasting or other powerful individuals and entities hoarding their attention, and also has given them power of knowledge previously available only to governments and businesses. It has become tools for political equality and democracy for many around the world. In the words of one highest court, "[The] Internet, rapidly spreading and reciprocal, allows people to overcome the economic or political hierarchy off-line and therefore to form public opinions free from class, social status, age, and gender distinctions, which make governance more reflective of the opinions of people from diverse classes and thereby further promotes democracy. Therefore, anonymous speech in the Internet, though fraught with harmful side-effects, should be strongly protected in view of its constitutional values."[1]

Given its relationship to democracy and human rights, it is only dialectically befitting that the first major Internet shutdown threatening democratization movements also took place during the Egypt uprising in 2011.[2] Increasingly, successive regimes have resorted to Internet shutdowns or blockage of major social media platforms, from 75 in 2016, 106 in 2017, 196 in 2018,[3] and 213 in 2019[4] a majority of which has been enacted for the actual purpose of most of them for suppressing communications during political protest or instability, military actions, or elections.[5]

Their impact is beyond political. "People routinely depend on the Internet to stay in touch with family and friends, create local communities of interest, report public information, hold institutions accountable, and access and share knowledge".[6] Also economies suffer greatly: Brookings Institute estimated the impact on the combined GDP of 19 countries practicing Internet shutdowns to be 2.4 billion USD between June 2015 and June 2016, working back from the countries of GDP figures and the estimated percentage of contribution from Internet,

---

[1] Korean Constitutional Court, 2010 Hun-ma 47, August 2012.

[2] http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html

[3] https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/

[4] TARGETED, CUT OFF, AND LEFT IN THE DARK, The #KeepItOn report on internet shutdowns in 2019 available at https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

[5] Id., and The State of Internet Shutdowns around the World: The 2018 #KeepItOn Report available at https://www.accessnow.org/cms/assets/uploads/2019/06/KIO-Report-final.pdf

[6] Internet Society, Internet Shutdowns: An Internet Society Public Policy Briefing, December 2019.

mobile, and major apps.[7] The impact on social, cultural, and educational rights are far-reaching.[8]

In this report, we will examine the laws enabling such Internet shutdowns or platform blockings and their validity under international human rights law and make recommendations. The focus will be on the *laws* rather than actions as the goal is to advise the legislators and adjudicators on the role of the laws enabling such shutdowns and blockings.

The state actions restricting specific online content or *unilateral* "media outlets" will not be covered here as their impact and coverage is not system-wide -- although one does albeit rarely find massive granular, content-specific censorship emulating the similarly comprehensive impact.[9] However, as we shall see later the *laws* enabling content-specific blocking are indistinguishable from the laws enabling blocking of interactive platforms, and will be covered as such. Although this report will focus on the cases of Asia Pacific as it will seek an international standard that can be applied universally, it will cover jurisprudence from all parts of the world, especially hard-to-seek court cases on internet shutdowns.

II. Domestic Laws and Practices

A. Overview of the Laws

1. Methodology

The Global Network Initiative's Country Legal Frameworks Resources, covering 53 major countries, catalogue the laws enabling Internet shutdowns and website blockings.[10] The Freedom House's Freedom on Net Country Reports provide information on how and whether 66 countries have engaged in Internet shutdowns and platform blockings. For the purpose of this report, we reviewed 2017 report and 2018 report of the Freedom on the Net. (Although the 2019 report came out while this report was being prepared, our focus is on the laws as opposed to the practices, which move slowly through the legislative process.) These two sets of documents covering 94 countries together will be the basis for our research.

2. Shutdown-enabling laws

---

[7] Brookings Institute, "Internet Shutdowns Cost 2.4 Billions Last Year", October 2016 https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf ; See also CIPESA, Economic Impact of Internet Disruptions in Sub-Saharan Africa, September 2017 (employing similar methods as the Brookings Institute for 10 African countries), https://cipesa.org/2017/09/economic-impact-of-internet-disruptions-in-sub-saharan-africa; Deloitte, The economic impact of disruptions to Internet connectivity, October 2016, https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf (using similar methods as Brookings but granulating for different levels of connectivity); EXX Africa, Special Report: The Cost of Internet Shutdowns in Africa, https://www.exxafrica.com/special-report-the-cost-of-internet-shutdowns-in-africa;

[8] Disconnected: A Human Rights-Based Approach to Network Disruptions. Global Network Initiative. June 2018. https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf

[9] Korea Communication Standards Commission was capable of taking down either by blocking or deleting 252,166 URLs in 2018. http://transparency.or.kr/notice/2509

[10] Global Network Initiatives, https://clfr.globalnetworkinitiative.org/

Network shutdowns are instituted by network operators, wired or wireless, usually by communication ministries of the country. The network operators or Internet Service Providers (ISPs) are almost always under the licensing by the state because mobile carriers require exclusive bandwidth licenses lest air waves do not interfere with one another and wired carriers require easement through underground conduits and on public electric poles through which broadband lines are installed. In exchange of these licenses on public properties, ISPs are imposed heavy regulatory frameworks under which they owe public interest obligations to cooperate with government requests under various justifications such as 'national security', 'combating illegal material', 'public security', 'regulatory compliance', 'conditions of license', etc. Also, these regulatory authorities include the powers to take down content in varying levels of granularity from license forfeiture (equivalent to national shutdowns), regional shutdowns, website blockings, and webpage blockings. To be specific, ISPs may lose licenses and thereby end up shutting down their entire networks for not blocking certain websites or webpages.

Since compulsion exercised upon network operators come through the general regulatory structure of each country's telecommunication regulations, most shutdown and blocking requests are made by telecommunication regulators almost always *without judicial process* and very often *without internal appeal process* although the right to constitutional challenges and other *external* forms of judicial review through administrative courts *after the fact* are made available by the general judicial system. Where the laws require judicial process for shutdown or blocking requests or make available internal appeal processes, those laws will be separately noted below.

Note: Although the same regulatory framework is often used to effect regional shutdowns around exam sites and prison sites, the laws enabling *only* those shutdowns, if at all, will not be covered since they are clearly not related to media freedom. However, it is most often through the aforesaid ordinary license regulatory scheme that various shutdown orders and requests are given to ISPs.

Albania (civil emergency[11]; license condition[12]; national protection of security and public order[13], law violation[14])

Australia (license condition(fee); individual threatening personal injury[15])

Bahrain (license condition[16])

Bangladesh (license condition(refusal to block)[17])

Belgium (public security[18])

---

[11] Law No. 8756

[12] Article 76 of Electronic Communications Act

[13] Article 113 of Electronic Communications Act

[14] Article 134 of Electronic Communications Act

[15] Section 315 of Telecommunications Act 1997

[16] Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites."

[17] Article 45 of Information and Communication Technology Act 2006

[18] Article 4 of the Electronic Communications Act

Brazil (illegal material[19])

Bulgaria (terrorism, national security;[20] martial law[21])

China (nationally owned, discretionary[22]; terrorism[23]; cybersecurity[24])

Colombia (regulatory violation[25])

Czech (cyber security[26])

DR Congo (public communication services, public security, national defense[27]; license conditions[28])

Egypt (national security[29])

El Salvadore (extortion, to be confirmed by court within 72 hours)[30]

Ethiopia (nationally owned, discretionary[31])

France (regulatory violation[32])

Germany (regulatory violation[33], public security[34])(appeal)

Ghana (war[35])

---

[19] Articles 7, III and 10(2) Law 12.965/14

[20] Law on Electronic Communications 2007, Article 301, paragraph 3

[21] Law on Electronic Communications 2007, Article 302 and Article 120 (radio spectrum suspension)

[22] all internet service providers obtain connection to the overseas internet through the gateways operated by a government agency Ministry of Industry and Information Technology (MIIT). CNNIC, 中国互联网络发展状况统计报告 [The 31st Report on the Development of the Internet in China], 21 (FON)

[23] Counter-Terrorism Law (2015)," China Law Translate, December 27, 2015 (FON), http://bit.ly/2eZydih

[24] Articles 12, 47, 68 of Cybersecurity Law of 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[25] Articles 64 and 65 of Law 1341 of 2009

[26] Act No. 181/2014 Coll. on the Cyber Security

[27] Article 46 of the Telecommunications Framework Law No. 013/2002

[28] Article 42 and 50 of Telecommunications Framework Law No. 013/2002

[29] Article 67 of the Telecommunications Regulation Law (No. 10 of 2003)

[30] Special Law Against Extortion Article 13

[31] The Ethio Telecom and the Ethiopian Telecommunication Agency (ETA) have exclusive control of Internet access throughout the country. https://en.wikipedia.org/wiki/Internet_in_Ethiopia

[32] Article L36-11 of the French Code of Post and Electronic Communications

[33] Section 126 of the German Telecommunications Act

[34] Section 115 of the German Telecommunications Act

[35] Section 99(6) of the Electronic Communications Act 2008 (Act 775)

Greece (public order, security and health[36]; public interest[37])

Honduras (None)

Hungary (unexpected attacks, preemptive defense, emergency, national crisis[38])

India (public emergency, public safety [39])

Ireland (terrorism[40]; license condition, public safety, security, or health threat[41])

Iran (license conditions, failure to block[42])

Italy (administration of justice[4344], intelligence agency's request[45], cyber crisis[46])

Jordan (crimes, security (also through court))[47]

Kazakhstan (crime, elections, extremism, terrorism;[48] license violation (through court);[49] emergency[50])

Kenya (state of emergency[5152])

---

[36] Article 3(a) of Law 4070/2012

[37] Article 20(9)(c) of Law 4070/2012; Article 14(2) of EETT's Regulation on the Use and Assignment of Rights for the Use of Radio Spectrum (radio spectrum suspension)

[38] Act CXIII of 2011 on home defense, Military of Hungary, and the implementable measures under special legal order, Art. 68, par. 5. Freedom On the Net Reports 2017–2018

[39] Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 under the Indian Telegraph Act, 1885

[40] Sections 20 to 29 of the Criminal Justice Act 2013

[41] Regulation 16(12), 17(1) European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2011 SI 335/2011

[42] Every ISP must be approved by both the Telecommunication Company of Iran (TCI) and the Ministry of Culture and Islamic Guidance, and must implement content-control software for websites and e-mail. ISPs face heavy penalties if they do not comply with the government filter lists. At least twelve ISPs have been shut down for failing to install adequate filters. Reporters Without Borders. "Report on Iran" Archived February 24, 2008, at the Wayback Machine.

[43] Article 96 of Legislative Decree No. 259 of 2003 (Electronic Communications Code)

[44] Article 348, paragraph 4 of the Criminal Procedure Code

[45] Article 13(1) of Law No. 124 of 2007

[46] Article 11 of Decree of the Prime Minister of 24 January 2013

[47] TELECOMMUNICATIONS LAW (NO. 13) OF 1995 AS AMENDED

[48] Article 41-1 of Law of the Republic of Kazakhstan on Communication No. 567-II Dated 5 July 2004

[49] Article 802 of Code of the Republic of Kazakhstan on Administrative Offences NO. 235-V Dated 5 July 2014

[50] Article 14-1 of Law of the Republic of Kazakhstan on Emergency Situations No. 387-II Dated 8 February 2003

[51] Article 58 and Article 132(4) of the Constitution of Kenya

[52] Royal Media Services Limited vs. The Hon. Attorney General,The Minister of Information and Broadcasting and the Communications Commission of Kenya [Petition No. 59 of 2013 High Court of Kenya]

Lesotho (national security or public order[53])

Malawi (public order, national security[54])

Malaysia (discretionary, license condition[55])

Malta (public emergency[56])

Mexico (criminal offences[57])

Montenegro (none, only under court decision[58])

Mozambique (state of siege or emergency[59])

Myanmar (license conditions)[60]

Netherlands (exceptional circumstances (usually war, terrorism, natural disaster etc)[61]

New Zealand (None)

Norway (None)

Pakistan (crimes ("misuse of services")[62], licence conditions[63], declaration of a state of emergency by the President of Pakistan, a time of war or of civil unrest[64])

Paraguay (None)

Portugal (siege or emergency[65] , serious and immediate threat to public security or health, or cyber security[66])

---

[53] Section 20 of the Communications Act 2012

[54] Article 24 of Electronic Transaction and Cyber Security Act, Freedom on the Net Report 2019

[55] Communications and Multimedia Act 1998

[56] Chapter 178 of the Emergency Powers Act

[57] Article 190(VII) of the Federal Telecommunications and Broadcasting Law (FTBL) and the Guidelines

[58] Enforcement and Security Act

[59] Articles 10 and 37 of Decree N.33/2001 of 6 November

[60] Section 22 of the Notification regarding TELECOMMUNICATIONS LAW 2013

[61] Article 14.4 of the Telecommunications Act

[62] section 21(4)(f) PAKISTAN TELECOMMUNICATION RE-ORGANISATION ACT (PTA) 1996

[63] section 9 PAKISTAN TELECOMMUNICATION RULES (PTR)

[64]54(2) of PTRA

[65] Constitution for the Portuguese Republic and Law No. 44/86 of 30 September, Articles 19, 134 and 138 of the Constitution of the Portuguese Republic and Law No. 44/86 of 30 September

[66] Articles 110 and 111 of the Electronic Communications Law

Qatar (national security, public emergency[67], license condition[68])

Romania (public interest[69], license violation[70])

Russia (terrorist activities, war[71])

Rwanda (national sovereignty[72])

Serbia (None)

Singapore (public interest, public morality, public order, public security, national harmony[73])

South Africa (emergency[74], regulatory violation[75])(appeal[76])

Spain (state of alarm, emergency and siege[77]; license violations[78], national defence, public security and civil protection[79])

Sweden (None)

Tanzania (license conditions[80] [81])

Thailand (None)

---

[67] Article 59 of Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law

[68] Article 3,4 and 12 of Decree Law No. (34) of 2006 on the promulgation of the Telecommunications Law, Article 15 of Decree Law No. (1) of 2009 on the promulgation of the Executive By-Laws for the Telecommunications Law

[69] Article 9(2) of the Government Emergency Ordinance No. 111/2011

[70] Article 147, 148 of the Government Emergency Ordinance No. 111/2011

[71] Article 6 of Federal Law No. 126-FZ Dated 7 July 2003

[72] Article 126 fo Law 24/2016 Governing Information and Communication Technologies

[73] Section 2, Internet Code of Practice, IMDA and Section 12 (1) of the Broadcasting Act, Freedom on the Net Report 2017-8

[74] Section 37 of the Constitution

[75] Electronic Communications Act No.36 of 2005 and Independent Communications Authority of South Africa Act No.13 of 2002

[76] Appeals are made to Inspector General of Intelligence.

[77] Organic Law 4/1981 of 1 June, on the State of Alarm, Emergency and Siege

[78] Article 79 and 82 of the General Telecommunications Act 9/2014

[79] Article 28.1 of The General Telecommunications Act 9/2014, Articles 17 and 53 of the Royal Decree 424/2005

[80] Regulation 36, Electronic and Postal Communications (Licensing) Regulations of 2011

[81] Under Section 163 of the Electronic and Postal Communication Act of 2010, a police officer or employee authorised by the Tanzania Communications Regulatory Authority may seize network equipment where he or she has reasonable grounds to believe that the electronic communication system supported by that equipment contravenes the terms of the licence issued to it by the TCRA or is otherwise in breach of the 2010 Act (or any regulations made under the Act). If no prosecution follows a seizure, the network equipment can be re-claimed within two months of the date of seizure or it is deemed forfeited.

Turkey (war, mobilization, public emergency[82], national security[83], public order[84], license conditions[85])

United Kingdom (public safety, public health, national security[86], civil protection[87], emergency power[88]

United States (None)[89]

Out of 55 countries surveyed, 21 countries have "license condition", "regulatory violation" as the most frequent bases for shutdowns. What is included here is the countries that own all the major ISPs.

18 countries list "national security", "public safety", "national integrity", "civil protection", "public order", "public interest" or similarly vague reasons as the second most frequent bases for shutdowns.

9 countries list "war", "emergency", "terrorism", "injury" and similarly narrow reasons as the third most frequent bases for shutdowns, while not allowing broader bases for shutdown such as "national security", "public safety", etc.

8 countries list "crimes", "illegal activities", "administration of justice", "refusal to block illegal information" and similar reasons as the bases for shutdowns

8 countries have no bases for shutdowns.

Only Montenegro and El Salvardo require judicial approval for all shutdowns while Kazakhstan and Jordan require court approval for part of the shutdowns.

Also, only South Africa and Germany allowed internal appeal by ISPs against shutdown orders while most countries allow ordinary administrative lawsuits or constitutional challenges against shutdowns mostly after they are instituted.

2. Blockage-enabling laws

Many countries allow the same network-shutdown authorities to block websites selectively for national security, illegal material, public security, etc., for the same litany of euphemisms. Often the same provisions enabling shutdown of an operator will logically and implicitly include the power to order blocking of particular websites.

---

[82] Article 34, Regulation on Information and Communication Technologies Authority Administrative Penalties

[83] Article 31, Regulation on Information and Communication Technologies Authority Administrative Penalties

[84] Article 32, Regulation on Information and Communication Technologies Authority Administrative Penalties

[85] Article 9, Electronic Communications Law

[86] Section 132, Communications Act 2003

[87] Part 1, Civil Contingencies Act 2004

[88] Part 2, Civil Contingencies Act 2004

[89] SEC. 204. [47 U.S.C. 204] HEARING AS TO LAWFULNESS OF NEW CHARGES; SUSPENSION concerns only "new charges. . . . and practices. Also, SEC. 9. [47 U.S.C. 159] REGULATORY FEES. concerns only failure to pay license fees.

In this chapter, we will catalogue the provisions explicitly enabling such selective measures because those provisions may represent more pernicious (though admittedly less system-wide) restrictions on press freedom than the shutdown provisions implicitly enabling such specific blockage. It is natural that the reasons for website blocking as opposed to Internet shutdown are more granular, e.g., child protection, intellectual property, gambling, pornography and other reasons, may not be related to media freedom but the consequences are the same.

Also, some of the website blockings are not instituted by the communication ministries' powers over ISPs but through courts' direct authorities over website operators.

Albania (crimes[90])

Armenia (crimes[91])

Australia (threat to personal injury[92])

Azerbaijan (danger to state and society[93])

Bangladesh (deterioration in law and order, hostility against other persons, prejudicial to State image, etc.)[94]

Bahrain (hatred of government, official religion, ethics, public peace)[95]

Belarus (crime)[96]

Belgium (illegal content)[97]

Brazil (illegal content(court))[98]

Bulgaria ('competent authority's request';[99] terrorism[100])

---

[90] Electronic Communications Act, as interpreted

[91] Article 11 of the Law on Police, Freedom house report 2018, p.7, "Episode of Satirical Web Series Removed from YouTube After a Complaint from Armenian Police," ePress.am, May 26, 2015, http://bit.ly/1MPFw6F(FON)

[92] Section 315 of Telecommunications Act 1997

[93] Mapping media freedom, Index on Censorship, https://mappingmediafreedom.ushahidi.io/posts/21726

[94] Articles 57, 59 of Information and Communication Technology Act 2006

[95] articles 19 and 20 of the Press Rules and Regulations, Decree—by—Law No. 47 Regarding organizing the press, printing and publishing [in Arabic], October 23, 2002, https://bit.ly/2welijt (FON)

[96] Ruling of the Operational and Analytical Center and the Ministry of communication and informatization № 6/8 from February 19, 2015, [in Russian]; "Amendments to the Law on Mass Media: registration of Internet publications, identification of commentators, blocking of social networks" [in Russian], Belarusian Association of Journalists, April 6, 2018. (FON)

[97] Chapter VI of Book XII of the Economic Law Code the Law of the Electronic Economy

[98] Articles 7, III and 10(2) Law 12.965/14

[99] Law on Electronic Communications 2006, Article 15(b) and Article 16, paragraph 2 (related to providers of caching or hosting services)

[100] Counter-terrorism Law 216

Cambodia (license condition)[101]

Colombia (data subject's rights[102])

Cuba (national integrity[103])

Czech (crimes[104], cyber security[105])

Denmark (only through court decision)[106]

DR Congo (public communication services, public security, national defense[107]) [108]

Egypt (terrorism[109], crimes[110](also through court))

France (terrorism[111])

Germany (illegal[112])(appeal)

Ghana (war[113])

Greece (public order, public health, public security, national defence, consumer protection,[114] hate speech[115])

Honduras (crimes[116])

India (public order, national integrity and security, foreign relations, defense, incitement(also through court))[117]

Indonesia (public order, anti-Islam, violation of laws or social norms, LGBT[118])

Iran (anti-Islam, anti-government)[119]

---

[101] 2015 Law on Telecommunications, Art. 24, https://bit.ly/2uGU7NL. (FON)

[102] article 21 of Law 1581 of 2012

[103] http://www.cubademocraciayvida.org/web/article.asp?artID=13302

[104] Section 8(1) of the Criminal Procedure Code.

[105] Act No. 181/2014 Coll. on Cyber Security

[106] Gaming Act 2016

[107] Article 46 of the Telecommunications Framework Law No. 013/2002

[108] Telecommunications Framework Law No. 013/2002

[109] 2015 Antiterrorism law

[110] Criminal Code

[111] Law No. 2014-1353 of 13 November 2014

[112] Section 59(3) of the Interstate Broadcasting Treaty

[113] Section 99(6) of the Electronic Communications Act 2008 (Act 775)

[114] Article 2(4) of Presidential Decree 131/2003

[115] Presidential Decree109/2010 (on-demand video services)

[116] CRIMINAL PROCEDURE CODE (DECREE 9-99-E)

[117] Section 69A of the Information Technology Act 2008 (IT Act)

[118] Information and Electronic Transactions Law(ITE LAw), Law No. 11/2008, Article 40.

[119] FON

Italy (crimes[120][121](also through court))

Jordan (violation of law[122])

Kazakhstan (hate speech, pornography, national integrity and security, extremism, and terrorism[123]; crimes[124])

Kenya (state of emergency or public security[125])

Lesotho (none[126])

Malawi (public order, national security[127])

Malaysia (seditious publication[128])

Malta (none, only under the Emergency Powers Act[129])

Mexico (none[130])

Montenegro (none, only under court decision[131])

Mozambique (none)

Myanmar (public interest and approval of government[132])

Netherlands (exceptional circumstances (usually war, terrorism, natural disaster,etc)[133])

New Zealand (None, only for child exploitation filtering)

Norway (crime[134])

---

[120] Legislative Decree No. 70 of 2003

[121] Criminal Procedure Code (Royal Decree No. 1398 of 1930)

[122] Press and Publications Law, Article 48 and Article 49

[123] Article 13 of Law of the Republic of Kazakhstan on Mass Media No. 451-1 Dated 23 July 1999

[124] Chapter 36-6 of Criminal Procedural Code of the Republic of Kazakhstan No. 231-V Dated 4 July 2014

[125] Section 3 of the Preservation of Public Security Act (Chapter 57) (the PPS Act)

[126] The government in Lesotho does not have the legal authority to order a network provider to block URLs or IP addresses, but under Section 5(3)(b) of the Emergency Powers Order 1988, the Minister may, during a declared state of emergency, issue related regulations.

[127] Article 24 of Electronic Transaction and Cyber Security Act

[128] Section 10 of Sedition Act 1948

[129] Chapter 178 of the Emergency Powers Act

[130] Although there are no specific provisions of blockings, the FTBL promotes net neutrality with Articles 145 and 146 of the Federal Telecommunications and Broadcasting Law (FTBL)

[131] Enforcement and Security Act

[132] Section 77 of the TELECOMMUNICATIONS LAW 2013

[133] Article 14.4 of the Telecommunications Act

[134] CRIMINAL PROCEDURE ACT 1981 216b CPA

Pakistan (information which is considered false, indecent or obscene[135], Anti-Islam, public order and decency, contempt of court[136])

Paraguay (crime[137])

Portugal (public health, public safety, national safety and defense, consumers, human dignity, public order, protection of minors, hate speech regarding race, sex, religion, nationality, crime)[138]

Qatar (national security, public emergency)[139]

Romania (illicit content[140])

Russia (child sexual abuse, drugs, suicide, victims under 18, illegal activity[141], illegal online information(also through court[142])[143])

Rwanda (national sovereignty[144])

Serbia (None)

Singapore (pornography, cults, violent crime, criminal skills)[145]

South Africa (None)

Spain (public security, public health, fundamental rights, child protection, intellectual property rights[146] (through court))

Sweden (crimes[147], consumer protection[148], intellectual property rights[149])

---

[135] 31(d) of PTRA
[136] section 37 PREVENTION OF ELECTRONIC CRIMES ACT (PECA) 2016
[137] LAW OF JUDICIAL ORGANISATION (LAW 879/1981)
[138] Decree-Law 7/2004 of 7 January (Portuguese Electronic Commerce Law)
[139] Article 59 of Decree Law No.(34) of 2006 on the promulgation of the Telecommunications Law
[140] Article 11(2) of Law No. 196/2003
[141] Article 15.1 of Federal Law No.149-FZ Dated 27 July 2006
[142] FON 2019
[143] Decree No.1101 of 26 October 2012 on the Unified Registry of illegal online information
[144] Article 126 of Law 24/2016 Governing Information and Communication Technologies
[145] Undesirable Publications Act
[146] Article 11.1, Article 8.1, Act 34/2002 of 11 July on Information Society Services and Electronic Commerce
[147] Chapter 27, Section 19, CODE (1942:740) OF JUDICIAL PROCEDURE
[148] Chapter 7, Section 9a, Electronic Communications Act 2003 (2003:389)
[149] In a recent judgement delivered by the Swedish Patent and Market Court of Appeal on February 13 2017, the court declared that an internet service provider that acts as an intermediary can be ordered to block access to websites that infringe intellectual property rights. As a consequence, the court issued an injunction, combined with a conditional fine, that required the internet service provider to block subscribers from accessing illegal streaming and piracy websites.

Tanzania (obscene material[150])

Thailand (national security, public order, good morals[151], violation of the dignity of the Monarchy[152])

Turkey (illegal content[153], national security and public order[154])

United Kingdom (terrorism[155])

United States (illegal activities(domain seizure))[156]

Out of 57 countries, 26 countries have "crimes', "violation of law", and "illicit/ illegal content", and "illegal activities" as the most frequent bases of website blocking. Note that these were only the fourth most frequently used bases of shutdowns. The most frequent bases for shutdowns, the licensing condition violation, does not apply to website blocking, since the latter is taken against a website operator and is not caused by ISP's behavior. As expected, in general, the reasons for blocking particular websites are more granular than the reasons for shutting down the Internet.

15 countries list "national security", "national integrity", "national sovereignty", "public order", "public interest" as the second most frequent bases of website blocking. This was the second most frequently cited bases for shutdowns.

Also, 12 countries list "war", "emergency", "terrorism", "injury", "defense', and other physical harms as the third frequently cited basis of website blocking.

Uniquely for website blocking, 5 countries list "anti-government", "violation of dignity of monarchy", "seditious publication", and "image of the state" as the basis of website blocking". The nature of website blocking as a discipline against a website operator is such that legal provisions are crafted to apply narrowly to certain content served on the Internet.

There are other less frequently appearing bases for website blocking such as intellectual property rights, child protection, pornography, and hate speech.

As expected, there are more court-based procedures (7 countries) for website blockings than shutdowns (2 countries). Website blocking is a disciplinary measure against website operators who are typically not licensed entities and therefore deserve more procedural safeguards than the typically licensed ISPs subject to close regulatory control.

As to administratively enforced actions, internal appellate procedure is still far between for website blocking as for shutdowns (only Germany).

---

[150] Section 45, Tanzania Communications Regulatory Authority Act 2003

[151] Section 20, Computer Crimes Act B.E. 2550 (2007)

[152] Section 2, Interim Constitution

[153] Article 9, Law No. 5651 on Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications

[154] A new omnibus law published recently provides the Chairman of the Presidency of Telecom Communications Head Office (TIB) with the power to request the blocking of websites and content in order to protect national security and public order, as well as to prevent crime.

[155] Section 3, Terrorism Act 2006

[156] 18 U.S.C. section 2323 (intellectual property infringements), 18 U.S.C. section 921 (money laundering)

The number of countries lacking website blocking authority altogether is even smaller (5 countries) than those lacking internet shutdown authority (8 countries). Given that the most prevailing bases for blocking is criminal or illegal online content or activity, it would be easier to justify such actions targeting specific websites.

B. Examples of Abuse in Application in Indo-Pacific : 2017-2019

In **China**, all internet service providers obtain connection to the overseas internet through the gateways operated by a government agency Ministry of Industry and Information Technology (MIIT)[157] which can cut off internet users from all or parts of the internet as in Xinjiang and Tibet.[158] On top of internet shutdown, there are laws and practices that target individual websites and contents.

An anti-terrorism law passed in 2015 (Article 48) imposes fines and detentions of up to 15 days on telecommunications operators and internet service provider (ISP) personnel who fail to "stop transmission" of terrorist or extremist content, "shut down related services," or implement "network security" measures to prevent the transmission of such content.[159] Also, the new cybersecurity law effective since June 2017 also empowers officials to order network operators to stop transmission of certain content to protect public security.[160]

Between 2015 and 2017, more than 13,000 websites have been blocked or closed according to a government count[161], mostly related to "health and safety, followed by media censorship, official wrongdoing, foreign affairs, the reputation of the party or officials, and civil society activism."[162] Only a few major international sites, such as CNN English, Huffington Post, the Guardian, and the Washington Post, were not blocked as of mid-2018. A wide range of other websites that might provide information of interest to Chinese users are blocked as well, including those of human rights groups and international businesses. Several social media and messaging platforms are completely blocked in China, such as Google, Facebook, WhatsApp, YouTube, Flickr, Tumblr, Dropbox, Instagram, SoundCloud,

---

[157] CNNIC, 中国互联网络发展状况统计报告 [The 31st Report on the Development of the Internet in China], 21

[158] See Alexa Olsen, "Welcome to the Uighur Web," Foreign Policy, April 21, 2014, http://atfp.co/1jmJCYH; Qiao Long, "新疆皮山县对外通讯中断 一网民议论民族政策被警告", Radio Free Asia, February 16, 2017, http://www.rfa.org/mandarin/yataibaodao/shaoshuminzu/ql1-02162017115429.html; "Video of a Self-Immolation In Tibet Appears On The Internet," VOA, April 15, 2017, https://www.voatibetanenglish.com/a/3811393.html; "Police Increase Checks of Uyghur Smartphone Users in Xinjiang," Radio Free Asia, January 8, 2016, http://www.rfa.org/english/news/uyghur/police-increase-checks-of-smartphone-users-in-xinjiang-01082016133532.html

[159] Drew Foerster, American Bar Association, "China's Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law," May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; "Counter-Terrorism Law (2015)," China Law Translate, December 27, 2015, http://bit.ly/2eZydih

[160] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-lawpeoples-republic-china/; https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[161] "習近平築「網路長城」到底有多高？官員自爆封鎖超過一萬三千個網站," TechNews, December 27, 2017, https://technews.tw/2017/12/27/great-firewall-of-china/; https://www.reuters.com/article/us-chinainternet/china-closes-more-than-13000-websites-in-past-three-years-idUSKBN1EI05M

[162] Sarah Cook, https://thediplomat.com/2018/01/the-news-china-didnt-want-reported-in-2017/

WordPress, and Pinterest.[163]Most famously, Google was blocked for not agreeing to censor politically sensitive search results.

China shows a classic example of how vaguely defined "security" in various public safety laws and the publicly owned internet infrastructure can be abused to suppress cross-border information exchange and can be used to suppress media freedom in selected geographic areas.

In **India**[164], blocking of websites takes place under Section 69A of the Information Technology Act 2008 (IT Act) and a 2009 subordinate legislation called the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules ("Blocking Rules").[165] The Blocking Rules allow the central government to direct any agency or intermediary to block access to information when it is regarded as "necessary or expedient" in the interest of the "sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above."[166] Intermediaries failing to comply are punishable with fines and prison terms of up to seven years.[167] ISPs are not asked to inform the public of blocks and the Blocking Rules require that executive blocking orders be kept confidential.[168] In the *Shreya Singhal* case,[169] the Supreme Court upheld Section 69A and the Blocking Rules against constitutional challenges, finding safeguards adequate and texts narrowly constructed.[170] Indian courts have issued several blocking orders against the websites that are primarily engaged in businesses that infringe intellectual property laws.[171]As to shutdowns, in August 2017, the Government of India issued the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017[172] under the Indian Telegraph Act, 1885. Central

---

[163] Freedom on the Net 2018 Report: China", p. 6

[164] Compiled by Lee JeeHo

[165] Chinmayi Arun and Sarvjeet Singh, "Online Intermediaries in India," February 18, 2015, Berkman Center for Internet and Society at Harvard University, https://cyber.harvard.edu/node/98684.

[166] Section 69A(1), The Information Technology Act, 2008.

[167] Section 69A(3), The Information Technology Act, 2008. 원본 확인

[168] Rule 16, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

[169] Common Cause v. Union of India [W.P.(C) No. 21 of 2013]; PUCL v. Union of India [W.P.(Crl) No. 199 of 2013].

[170] Shreya Singhal v Union of India, (2015) 5 SCC 1.

[171] Star India Pvt. Ltd. v. Haneeth Ujwal & Ors., 2014 SCC Online Del 3837; Star India Pvt. Ltd. v. Roy Ma & Ors., 2014 SCC Online Del 2300; Fox Star Studios India Ltd. v. John Ceedge & Ors., 2014 SCC Online 1822; Novi Digital Entertainment Pvt. Ltd. & Anr. v. Five Desi & Ors. at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=176887&yr=2016 [https://perma.cc/8XKS-R333]; Star India Pvt. Ltd. vs. Khalid Nasir Raja & Ors., at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=59032&yr=2015 [https://perma.cc/LDM3-RPAG]; Star India Pvt. Ltd. v. Sujit Jha & Ors. at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=240702&yr=2014 [https://perma.cc/5DDN-VBWL]; Fox Star Studios India ltd. v. Macpuler William & Ors. at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=110404&yr=2015 [https://perma.cc/KJ5Z-LQ33]; In one such case, the Department of Technology appealed against the preliminary injunction as being overbroad. The appeal was dismissed by the appellate court applying similar principles as the UK courts. This court emphasised the importance of showing overwhelming evidence of infringement (Department of Electronics & Information Technology v. Star India Pvt. Ltd. at http://lobis.nic.in/ddir/dhc/PNJ/judgement/29-07-2016/PNJ29072016REVIEWPET1312016.pdf [https://perma.cc/BQ77-43BD]

[172] Dot.gov.in. (2019). Available at: http://dot.gov.in/sites/default/files/Suspension%20Rules.pdf

and state governments follow these rules to issue shutdown orders. If the central government issues an order, it comes from the Secretary in the Ministry of Home Affairs, and if a state orders it, it comes from the Secretary to the State Government. The Superintendent of Police or an officer of equivalent rank directs the service provider to carry out the order. Prior to the introduction of these rules, the government relied on Section 144 of the Code of Criminal Procedure, under which the District Magistrate had been authorized to issue shutdown orders.

India has become a global leader in the number of internet shutdowns. Local governments routinely shut down the internet during protests, violence, examinations, and even festivities.[173] Shutdowns were implemented in at least 14 states in 2018[174] in varying duration from a few hours to a few days. In September 2018 in Rajasthan after three men were murdered, the Internet was shutdown to prevent misinformation and hate speech.[175] India's case demands attention because the numerous shutdowns are not directed at suppressing media freedom or maintaining dictatorship but are justified as precautionary measures to contain the otherwise 'unruly' public as perceived. Again, India's case calls for an examination into the process by which shutdowns are enacted and who makes those decision in

In **Cambodia[176]**, the goal of the Telecommunications Regulator of Cambodia (TRC), the main regulatory body, is to regulate the operations of telecommunications networks and services to "*promote fair, efficient, and transparent competition*."[177] The independency of the TRC was largely weakened under the 2015 telecommunications law.[178] An example of its lack of independence was a block on the Cambodia Daily in September 2017, which was well-known for having disclosed corruptions scandals and human rights abuses in Cambodia.

There were other websites shut down before general elections in July 2018, which contributed to the victory of Prime Minister Hun Sen and the CPP.[179] Blocking is implemented on websites presenting pornography and sexually explicit images.[180] There is an inter-ministerial "prakas" or proclamation issued by the government in May 2018, which can

---

[173] Sarvjeet Singh, "Incidents of Internet Shutdowns in India (2010 onwards)", Centre for Communication Governance at National Law University, Delhi, https://drive.google.com/file/d/0BycAZd9M5_7NOExCRnQ3Q1pqcm8/view.

[174] Sarvjeet, supra

[175] https://timesofindia.indiatimes.com/city/udaipur/triple-murder-inside-hosp-premises-over-property-row-shocks-banswara/articleshow/65640390.cms

[176] Kim Dohui

[177] 'Background', *Telecommunications Regulator of Cambodia*, https://bit.ly/2G7SYUD.

[178] 2015 Law on Telecommunications, Art. 24, https://bit.ly/2uGU7NL.

[179] 'Cambodia blocks some independent news media sites: rights group,' Reuters. 27 July 2018, https://reut.rs/2LVruXP; Cambodia's ruling party claims victory in election condemned as 'neither free nor fair', CNN.com, 30 July 2018, https://cnn.it/2R8NGgM.

[180] Michael Dickinson, 'Ministry Seeking to Curb Sexual Images Online', *The Cambodia Daily*, 25 October 2016, https://bit.ly/2dGJDs3.

contribute to potential blocking and filtering of online content.[181] A code of conduct for media was issued by the NEC in May 2018 prior to the July elections.[182]

In **Philippines**[183], the National Telecommunications Commission (NTC) has authority of network shutdown. Mobile phone networks were blocked by the government during major events in several cities.[184] In January 2018, the online news network *Rappler* – which had been critical of Duterte – was ordered closed by the Securities and Exchange Commission for failing to comply with a rule limiting media ownership to Filipinos but it was not under any law allowing disruption with the access.[185]

Myanmar

In Myanmar, the Telecommunications Law, Article 77[186] includes provisions allowing the government to block and filter contents for 'benefit of the people'.

Though the government is infamous for its consistent shutdown and blockage, the shutdown of 2019 was the longest. 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 9 townships in Rakhine and Chin states in Myanmar at least for 71 days.[187] Despite the government's assertion of security and violence as the reasons, about 500,000 Rohingyas in the conflict regions were assumed to be the main target.[188]

Those who sought refuge in Bangladesh also have limited access on the net, as the Bangladeshi government is denying 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.[189]

Pakistan

---

[181] http://safenetvoice.org/wp-content/uploads/2018/06/20180604_Inter-Ministerial_Prakas_On_Social-Media.pdf (please check sources)

[182] Soth Koemsoeun, 'NEC warns Press of Elections', *The Phnom Penh Post*, 28 May 2018, https://bit.ly/2JPA7St; 'NEC Issues Press Release on Rights and Prohibitions for Media', *Fresh News*, 24 May 2018, https://bit.ly/2zMbe6f.

[183] Compiled by Kim Eui Yong

[184] Jhoanna Ballaran, "Group criticizes gov't move shutting down cellphone signals during events," Philippine Daily Inquirer, January 26, 2018, http://newsinfo.inquirer.net/963786/group-criticizes-govt-move-shutting-down-cellphone-signals-during-events-signal-jamming-cell-sites-fma-media-group-shutdown

[185] Carmela Fonbuena, "SEC orders Rappler to shut down," *Rappler*, January 15, 2018, http://www.sec.gov.ph/wp-content/uploads/2018/01/2018Decision_RapplerIncandRapplerHoldingsCorp.pdf

[186] Article 77 : The Ministry may, when an emergency situation arises to operate for public interest, direct the licensee to suspend a Telecommunications Service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications, and to temporarily control the Telecommunications Service and Telecommunications Equipments, http://www.burmalibrary.org/docs23/2013-10-08-Telecommunications_Law-en.pdf

[187] 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

[188] Freedom on the Net Report 2017, 2018, 2019, Myanmar

[189] Freedom on the Net Report 2019, Myanmar

Section 54 of the 1996 Pakistan Telecommunications Act grants authorities the power to suspend services, acting as grounds for shutdowns.[190] The written law firmly states that such action must be invoked only during a state of emergency, but in reality this section has been abused by the government as grounds for routine shutdowns.[191] Such action has prompted a number of court cases, making shutdowns a popular topic for legal debate.

Mobile and internet services were shut down in parts of Lahore before the general elections,[192] for the Ashura holiday.[193], peaceful protest regarding grassroots civil rights movement,[194] and also for 12th Rabiul Awwal[195], and during protests by right-wing groups regarding the Supreme Court acquitting Asia Bibi, a Christian woman accused of blasphemy.[196]

In February 2018, a drastic change happened in court as the Islamabad High Court (IHC) ruled that mobile network shutdowns and mobile-based internet suspension on grounds of public safety under Section 54(3) of the PTA, infringed the fundamental rights of

---

[190] Section 54. National Security. (1) Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorise any person or persons to intercept calls and messages or to trace calls through any telecommunication system.

(2) During a war or hostilities against Pakistan by any foreign power or internal aggression or for the defense or security of Pakistan, the Federal Government shall have preference and priority in telecommunication system over any licensee.

(3) Upon proclamation of emergency by the President, the Federal Government may suspend or modify all or any order or licences made or issued under this Act or cause suspension of operation, functions or services of any licensee for such time as it may deem necessary. Provided that the Federal Government may compensate any licensee whose facilities or services are affected by any action under this sub-section

[191] Freedom on the Net 2017, 2018, 2019, Pakistan

[192] "Nawaz Sharif's return prompts govt to suspend mobile phone, internet services", The News International, July 13, 2018, https://www.thenews.com.pk/latest/341267-nawaz-sharifs-return-prompts-govt-to-suspend-mobile-phone-internet-services

[193] The Ashura holiday is observed most visibly by the Shiite sect, which is a minority group in Pakistan and often the target of sectarian terrorist groups.; "Cellular networks jammed in different parts of country for 9, 10 Muharram", Pakistan Today, September 30, 2018, https://www.pakistantoday.com.pk/2018/09/20/mobile-phone-service-suspended-in-different-parts-of-country-for-9-10-muharram/

[194] "Pakistan shuts down the internet three times in one week", AccessNow, November 6, 2018, https://www.accessnow.org/pakistan-shuts-down-the-internet-three-times-in-one-week/

[195] "Cellular Services Suspended In Few Cities Today", AbbTakk, November 21, 2018, https://abbtakk.tv/en/cellular-services-to-remain-suspended-today/

[196] Freedom on the Net 2019 (citing "Mubasher Bukhari and Saad Sayeed, "Pakistan shuts phone networks as Islamists protest over Christian woman", Reuters, November 2, 2019, https://uk.reuters.com/article/uk-pakistan-blasphemy/pakistan-shuts-phone-networks-as-islamists-protest-over-christian-woman-idUKKCN1N7188")

Pakistani citizens and were thus illegal.[197] Unfortunately in March 2018, the judgement has been suspended and there still is no official court opinion.[198]

Regarding blockage of social media platforms, in November 2017, due to protests that were deemed violent, various social media platforms were suspended nationwide for two days.

In **Kazakhstan**, no government entity has the general power to order a network operator to shut down their network or subject them to a suspension of service, unless it "fails to comply with its obligations under other laws". Article 41-1 of the Communication Law stipulates that a network can be shut down or have its service suspended if it is used for criminal purposes, or if it is used to spread information which breaches Kazakhstan's laws regarding elections, extremism and terrorism.[199] To do this, the General Prosecutor or the Deputy Prosecutors must issue a prosecutor order to the Ministry of Investment and Development, which will proceed to shut down the network or access to its services.

Article 802 of the Administrative Offences Code stipulates that court proceedings can be brought against network operators if they fail to obey the requirements of their licences, or if their technicians have not met the required qualification requirements.[200] Individuals or businesses can submit evidence to the court regarding an offence that has been committed, and courts can order the termination or suspension of a network operator's licence. The Emergency Law provides for certain government entities the right to the priority usage of networks and the right to shut them down in emergency situations (article 14-1)[201].

The government has extensive authority to block online content in Kazakhstan. Although there is no specific provision in the law related to blocking IP addresses or web pages, article 13 of the Mass Media Law describes situations where the distribution of mass media products can be blocked or suspended, such as disclosing of state secrets, promoting of drug use, inciting racial hatred, or containing pornographic material.[202] Under Chapter 36-3 of the Criminal Procedural Code, individuals, businesses, prosecutors, and government entities can apply to the court to suspend or block access to foreign mass media under article

---

[197] Judgment reported as PLD 2018 Islamabad 243; "Islamabad High Court Ruled Mobile Network Shutdowns Illegal", Digital Rights Foundation, February 27 2018, https://digitalrightsfoundation.pk/islamabad-high-court-ruled-mobile-network-shutdowns-illegal/

[198] Rizwan Shehzad, "IHC allows cellular service suspension for time being", The Express Tribune, March 20 2018, https://tribune.com.pk/story/1665210/1-ihc-allows-cellular-service-suspension-time/

[199] International Service for Human Rights, "The situation of human rights Defenders: Kazakhstan", Human Rights Committee Briefing Paper- August 2015, https://www.ishr.ch/sites/default/files/article/files/situation_of_hrds_in_kazakhstan.pdf / Communication Law: https://online.zakon.kz/Document/?doc_id=1049207#pos=1212;-37&sdoc_params=text%3Dundefined&sdoc_pos=0

[200] Global Network Initiative, Kazakhstan, https://globalnetworkinitiative.org/clfr-kazakhstan/2/

[201] Global Network Initiative, Kazakhstan, https://globalnetworkinitiative.org/clfr-kazakhstan/2/

[202] Mass Media Law, Article 13. Suspension and termination of production of mass media or distribution of media products, http://adilet.zan.kz/eng/docs/Z990000451_#:~:text=The%20Law%20of%20the%20Republic%20of%20Kazakhstan%20dated%2023%20July%201999%20No.&text=This%20Law%20regulates%20public%20relations,of%20the%20Republic%20of%20Kazakhstan.

13 of the Mass Media Law. The court order will be executed by the Ministry of Investment and Development.[203]

In Kazakhstan[204], social media and communication platforms have been restricted during political events.[205][206] The government has repeatedly throttled or disconnected the internet in an effort to prevent political protests.[207] Websites, social media and communication platforms are routinely blocked pursuant to article 14 of the Emergency Law. Online content related to pornography, extremism, terrorism, or violence is the most frequently blocked, though political and social content istargeted as well. Blockages became more frequent after the opposition party, the Democratic Choice of Kazakhstan (DVK), was recognized as an extremist organization by the court.[208] Following March of 2018, the government has throttled internet access to social media platforms almost daily for approximately one hour, whenever Mukhtar Ablyazov, the leader of DVK was streaming on Facebook Live.[209] The regulator adopted a system[210] to monitor the online media,[211] and it is reported that there were approximately 270,000 takedown requests[212].

On June 9, 2019, Kazakhstan held an early presidential election. For several days, mobile internet services were interfered with and access to social media platforms including Facebook, Instagram, Periscope, and WhatsApp were blocked.[213] Services were completely blocked in areas where political protests were held, and in public parks. During anti government demonstrations on May 9, 2019, access to Facebook, Instagram, and YouTube was restricted for one day.[214] Over the course of May 2019, the authorities repeatedly restricted access to Facebook, Instagram, and YouTube. Access to Telegram was persistently restricted. Throttling of internet access returned in May 2019 as anti government

---

[203] Global Network Initiative, Kazakhstan, https://globalnetworkinitiative.org/clfr-kazakhstan/2/

[204] Chung Jae Wung

[205] Facebook, Instagram, YouTube, and Telegram users have reported difficulties to access during the coverage period.

[206] https://eurasianet.org/kazakhstan-is-throttling-the-internet-when-the-presidents-rival-is-online

[207] https://netblocks.org/reports/internet-and-streaming-services-blocked-in-kazakhstan-on-election-day-dAmOP7y9

[208] "MIC says it might block Facebook…" [in Russian] Informburo.kz, March 27, 2018, https://bit.ly/2EQJDy5 ; "Kazakhstan may block Telegram entirely"

[209] Keepit on report 2018 …..page 14(citing: Freedomhouse.org. (2019). Kazakhstan Country Report | Freedom on the Net 2018. Available at: https://freedomhouse.org/report/freedomnet/2018/kazakhstan)

[210] "Automated System of Monitoring the National Information Space."

[211] "Kazakhstan adopts rules for state monitoring of internet," [in Russian] Digital.Report, February 29, 2016, http://bit.ly/1SegFwe. [please check sources]

[212] "Control the internet...," [in Russian] Tengrinews.kz, November 8, 2017, http://bit.ly/2hVRu4X.; https://monitor.civicus.org/newsfeed/2018/01/31/kazakhstan-strikes-arrests-and-fears-new-restrictions-fundamental-freedoms/

[213] "Social media blocked in Kazakhstan on Victory Day", NetBlocks, May 9, 2019, http://bit.ly/2Vtk2bC https://www.rferl.org/a/rfe-rl-s-kazakh-website-other-sites-not-accessible-in-kazakhstan/29930391.html "Kazakh officials have not given an official explanation, and representatives of the Information Ministry, National Security Committee, and Kazakhtelecom were not available for comment". Therefore, there is no law invoked to justify the blockage.

[214] "Kazakhstanis did not complain about blocks," Kursiv.kz, May 15, 2019, http://bit.ly/336X9v3

demonstrations broke out across the country. Hosting websites including Archive.org, Issuu, LiveJournal, Reddit, Tumblr, and ustream.tv. were either intermittently or permanently unavailable.[215] SoundCloud was temporarily blocked in September 2018, for "carrying extremist and terrorist materials".[216]

In **Russia**, the authorities are able to shut down internet access pursuant to article 37 of the Federal Law No.126-FZ(the Law on Communications)[217] for the needs of the state administration, including of presidential and government communications, for the needs of the country's defence and of state security, as well as for ensuring law and order. In addition, in May 2019, the so-called "sovereign internet" law, which aims to rewire the Russian segment of the web in order to render it independent from the broader internet, was signed into law and is expected to centralize the Russian authorities' grip on information and communications technology infrastructure[218]. The law requires communication providers, owners of technological communication networks to provide information to the Federal Service for Supervision of Telecommunications, Information Technology and Mass Communication(Roskomnadzor) or to install hardware and software tools that enable Roskomnadzor to monitor traffic, including access to resources blocked in Russia.[219]

With these lawful regulations, authorities attempted to disrupt the internet not only in the Republic of Ingushetia, in the North Caucasus on at least eight occasions in 2018 and 2019[220], but also during the mass protests over a border agreement which ceded territory to the neighboring Republic of Chechnya in June, October and November 2019[221].

With regard to blocking or censoring contents online, Roskomnadzor is entitled to block or blacklist IP addresses and webpages that contain illicit contents and extremist activities under the Federal Law No. 149(Law on Information)[222] without a court order.

---

[215] The authorities have typically attributed disruptions to ill-explained technical issues. (https://bit.ly/2S3Rj6H); The authorities have typically attributed disruptions to ill-explained technical issues (https://twitter.com/aygeryma/status/1108387532474064896); The authorities stated that "technical work" being carried out as a result of this ruling could explain service interruptions to Telegram in particular. (https://bit.ly/2S7At7i)

[216] "Russian website removed extremist content", Sputniknews, September 29, 2018, http://bit.ly/2DEAVVk, "Popular websites complied with MIC requests", Informburo.kz, August 13, 2018, http://bit.ly/2UUKJRO

[217] article 37.2 of the Federal Law on Communications: The licensing body has the right to suspend the licence validity if:
1) violations are exposed which may entail infliction of damage upon the man's rights, lawful interests, life and health, or upon the provisions for the needs of the state administration, including of presidential and government communications, for the needs of the country's defence and of state security, as well as for ensuring law and order.

[218] Freedom On the Net Report 2019

[219] https://www.lexology.com/library/detail.aspx?g=ce0a08d6-bf55-4a19-8799-a7907e016cd8

[220] Freedom On the Net 2019(citing "https://www.vedomosti.ru/politics/articles/2019/03/24/797252-otklyuchen…; "The Internet in Ingushetia during the rallies was turned off at the request of the security agencies" [in Russian], RosKomSvoboda, November 15, 2018, https://roskomsvoboda.org/43042/")

[221] Freedom On the Net 2019(citing "https://www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS58_LEG_264.pdf")

[222] article 15.3 of the federal law No.149(Law on information): the federal executive governmental body shall send a demand via the interaction system to communication operators for taking measures for restricting access to the information resource, for instance to a website on the Internet or to the information that is placed on it and

Empowered with a broad jurisdiction, it may exercise this power on the basis of evidence it has found itself. It restricted, or has attempted to restrict many social media and communication platforms, including Telegram[223], Alibaba Cloud, Amazon Web Services, Google Cloud, and other social media platforms such as Viber and Odnoklassniki. Other messaging apps, such as Zello were blocked by Roskonmadzor in 2017 for refusing to hand over its encryption keys which would enable authorities to approach much of the service's data. BlackBerry Messenger, imo, Line, and Vchat were blocked for similar reasons in 2017.[224]

In **Bangladesh**, the authorities may issue an order to a license holder under section 45 of the Information and Communication Technology Act(ICT Act) to take certain measures or cease certain activities if it is necessary to ensure compliance with the provisions of the ICT Act or rules and regulations[225].

In fact, a number of internet shutdowns targeted connectivity during the elections and mass protests occurred in 2018. The BRTC(Bangladesh Telecommunication Regulatory Commission) restricted the 3G and 4G services several times in the run-up to the election and on election day[226].

Furthermore, under sections 57 and 59 of the ICT Act, the authorities may make an order to block the communication flow if any person deliberately publishes or transmits any material which can be regarded as false, cause deterioration in law and order, etc[227]. In practice, the government occasionally restricts access to social media and communication platforms when they are suspicious of being critical of authorities[228].

Before the national elections, the BTRC briefly blocked Skype in November 2018 to thwart communication between exiled leaders of the opposition and their activists. In 2015, Facebook, Facebook Messenger, WhatsApp and Viber were among several platforms temporarily blocked[229], while communications apps, Threema and Wickr were blocked from May 2016 into mid 2018 when intelligence agencies claimed that the apps were critical of Islam and responsible for the spread of atheism[230].

---

contains calls for mass disorders, pursuance of extremist activities, participation in mass (public) events conducted in breach of established procedure.

[223] Wikipedia (citing "Роскомнадзор начал процедуру блокировки Telegram - Экономика и бизнес". ТАСС(in Russian). Retrieved May 19,2018.)

[224] Freedom On the Net 2019(citing "https://xn--b1aew.xn--p1ai/news/item/15312380")

[225] Global Network Initiatives, https://clfr.globalnetworkinitiative.org/

[226] "Bangladesh: Internet throttled, journalists attacked during parliamentary elections", International Federation of Journalists, January 2, 2019, https://www.ifj.org/fr/salle-de-presse/nouvelles/detail/category/press-releases/article/bangladesh-internet-throttled-and-journalists-attacked-t-during-parliamentary-elections.html

[227] Global Network Initiatives, https://clfr.globalnetworkinitiative.org/

[228] "Internet Services to be suspended across the country", DhakaTribune, February 11, 2018, https://www.dhakatribune.com/regulation/2018/02/11/internet-services-suspended-throughout-country/

[229] "Social networking sites closed for security reasons, says Minister Tarana Halim," BDNews24, November 18, 2015, http://bdnews24.com/bangladesh/2015/11/18/social-networking-sites-closed-for-security-reasons-says-minister-tarana-halim; Ishtiaq Husain, "Twitter, Skype, Imo blocked in Bangladesh," December 13, 2015, http://www.dhakatribune.com/bangladesh/2015/dec/13/government-blocks-twitter-skype-and-imo; Agence France-Presse, "Bangladesh Lifts Ban on All Social Media," via Express Tribune, December 14, 2015, http://tribune.com.pk/story/1010061/bangladesh-lifts-ban-on-all-social-media/

[230] Muhammad Zahidul Islam, "Govt blocks 2 messaging services," May 20, 2016, http://www.thedailystar.net/frontpage/govt-blocks-2-messaging-services-1226884

Global trends

KeepItOn Report 2018 defines Internet shutdown as follows, including social media platforms, and therefore, the definition is compatible with this research:[231]

> An internet shutdown can be defined as 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."[3] They include blocks of social media platforms, and are also referred to as "blackouts," "kill switches," or "network disruptions."

Most internet shutdowns have taken place in India which cover 134 out of 196 in 2018 and 121 out of 213 in 2019. In OECD countries, you can find almost none showing the disproportionate impact the shutdowns are having on the less developed sectors.

Most shutdows are taking place in Asia and Africa, with the exceptions such as Turkey, Russia, and Venezuela although Brazil's famous *Whatsapp* blocking took place only too early to be added here.

The most worrying trend is lack of transparency about why the internet is shut down:

> [In 2018],. . . when governments shut down the internet citing "public safety [91 cases]," it is often evident to observers that, in reality, authorities may fear protests and cut off access to the internet to limit people's ability to organize and express themselves [one third (⅓)]. . . when authorities cite "fake news," rumors, or hate speech [33 cases], they are often responding to a range of issues including communal violence [20], protests[5], elections [4], political instability [3], among others. (numbers in bracket provided by this author)[232]

> [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."[233]

Also, in 2019, more than half of 24 shutdowns motivated by 'public safety' were actually attempts to quell protests while more than half of 30 shutdowns taken as precautionary measures were done to shutter people's criticism and knowledge of military actions. Again, fake news and hate speech cases (33) were also part of military actions, or responses to protests, and other community happenings.

In a stark example, post-election shutdown, ostensibly aimed at abating "fake news" about election results, turned out to be a cover-up for election rigging as in DRC.[234] More than one half of national security shutdowns (40) were actually responses to political instability.[235]

---

[231] KeepItOn 2018, page 3
[232] KeepItOn 2018, page 5
[233] KeepItOn 2019, page 3
[234] KeepInOn 2018,
[235] Id.

Actually, research has shown that internet shutdowns, ostensibly enacted to protect the public, often occur in conjunction with higher levels of state repression.[236] In 2018, there were at least 33 incidents of state violence reported during internet shutdowns. It appears that in some cases, governments and law enforcement may cut off access to the internet to unleash violence on citizens with impunity. In Sudan, protesters have become victims to state violence under the "cover" of shutdowns.

Moreover, even innocuous shutdowns affect the state's sensitivity to other shutdowns, KeepItOn Report states that, among the shutdown incidents between 2014-2018, "the countries that shut down the internet for exams are more likely to cut access during protests, elections, and for information control."[237]

Blocking specific social media platforms may be more pernicious in intent than taking down the whole Internet as in case of Venezuela:

> 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.[238]

Likewise, "geographically targeted shutdowns can be an especially obvious attempt at discrimination, exclusion, and censorship of voices speaking out against harmful government practices"[239] as in Myanmar's and Bangladesh's case on Rohingyas, India's case on Kashmir and Jammu, and Indonesia's case on Papua.[240]

III. Legal Analysis

United Nations

The UN Human Rights Committee warned about Internet shutdowns as early as 2011 in its seminal General Comment 34, setting up presumption of infringement on any broad restriction against an entire site or an entire system:

> 43. Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the

[236] Gohdes, Anita R. "Pulling The Plug Network disruptions and violence in civil conflict". Journal Of Peace Research, vol 52, no. 3, 2015, pp. 352-367. SAGE Publications, doi:10.1177/0022343314551398.
[237] KeepItOn 2018, page 7
[238] KeepInOn 2019, page 7
[239] KeepInOn 2019, page 5
[240] KeepInOn 2019, page 5-6

political social system espoused by the government. (citing Concluding observations on the Syrian Arab Republic (CCPR/CO/84/SYR))[241]

Also, the UN Human Rights Council have affirmed on four different occasions, almost once every 2 years since 2012, that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights."[242] That statement first uttered in 2012 and repeated afterwards put to rest the issue of whether new rights must be invented for the Internet.[243] This statement is highly relevant to Internet shutdowns because, in order to protect offline rights equally online, the Internet must be made available "as a precondition".[244] This is why the Human Rights Council in its first resolution of the kind in 2012 also "calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."[245] Four years later, when it was revealed that the access issue can arise also in the countries that already have internet access, the UN Human Rights Council finally "condemn[ed] unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures".[246]

In addition, the most explicit statements of guidance have come from the reports of the two successive UN Special Rapporteurs on Freedom of Expressions Frank La Rue and David Kaye whose focus was timely shifted to the freedom of expression in the digital space when the Human Rights Council's resolution emphasized on the freedom of expression as the offline right to be protected online equally.

Most relevantly, in his 2011 report which predates both the Human Rights Council's first Internet freedom resolution and the Human Rights Committee's General Comment 34, La Rue states that "[t]he Special Rapporteur is deeply concerned by increasingly sophisticated blocking or filtering mechanisms used by States for censorship. The lack of transparency surrounding these measures also makes it difficult to ascertain whether blocking or filtering is really necessary for the purported aims put forward by States. As such, the Special Rapporteur calls upon States that currently block websites (1) to provide lists of blocked

---

[241] *See* CCPR/C/GC/34, http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf [https://perma.cc/876X-JFF3]

[242] UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet : resolution adopted*, 5 July 2018, A/HRC/38/L.10/Rev.1, available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement; UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet : resolution adopted* 18 July 2016, A/HRC/RES/32/13, available at: https://www.refworld.org/docid/57e916464.html ; UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet : resolution adopted* 14 July 2014, A/HRC/RES/26/13, available at: https://www.refworld.org/docid/5583dfe64.html ; UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet : resolution adopted* 5 July 2012, A/HRC/RES/20/8, available at: https://www.right-docs.org/doc/a-hrc-res-20-8/ [accessed 12 March 2020]

[243] Matthias C. Kettemann, "UN Human Rights Council Confirms that Human Rights Apply to the Internet", European Journal of International Law Blog, July 23, 2012

[244] Id.

[245] *Human Rights Council*, supra, 5 July 2012, A/HRC/RES/20/8

[246] *Human Rights Council, supra*, 18 July 2016, A/HRC/RES/32/13

websites and full details regarding the necessity and justification for blocking each individual website. An explanation should also be provided on the affected websites as to why they have been blocked. (2) Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences.[247]"

In the same 2011 report, La Rue also states that: "While blocking and filtering measures deny users access to specific content on the Internet, States have also taken measures to cut off access to the Internet entirely. The Special Rapporteur considers "cutting off users from Internet access, regardless of the justification provided, . . . to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights." La Rule goes as far as calling "upon all States to (3) ensure that Internet access is maintained at all times, including during times of political unrest."[248] Here, La Rue was considering the so-called "three strike" laws of France, UK, and ACTA affecting a small number of individuals.[249]

In the report, La Rue explains as follows the absolute language he uses on Internet access:

> Very few if any developments in information technologies have had such a revolutionary effect as the creation of the Internet. Unlike any other medium of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents a significant leap forward as an interactive medium. Indeed, with the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information. Such platforms are particularly valuable in countries where there is no independent media, as they enable individuals to share critical views and to find objective information. . . More generally, by enabling individuals to exchange information and ideas instantaneously and inexpensively across national borders, the Internet allows access to information and knowledge that was previously unattainable. This, in turn, contributes to the discovery of the truth and progress of society as a whole."[250]

La Rue's main concern was the effects on the individuals cut off from the revolutionary communication facilities. Therefore, the reasoning applied to the cut-off of specific individuals as in the three-strike laws should be applicable to Internet shutdowns affecting a large number of people.

Finally, the UN General Assembly also resolved in its resolution adopted by consensus in 2017 on the Safety of Journalists and the Issue of Impunity[251]: "Condemns unequivocally measures in violation of international human rights law aiming to or that intentionally prevent or disrupt access to or dissemination of information online and offline, aiming to undermine the work of journalists in informing the public, and calls upon all States to cease and refrain from these measures, which cause irreparable harm to efforts at building inclusive and peaceful knowledge societies and democracies."

Europe

---

[247] Frank La Rue, 2011 Internet general report (Para 70)

[248] Frank La Rue, 2011 Internet report, Paras. 78-79

[249] Frank La Rue, 2011 Internet report, Paras. 49-50

[250] La Rue, 2011 Internet report, Para 19.

[251] UN General Assembly, Resolution on the Safety of Journalists and the Issue of Impunity, A/C.3/72/L.35/Rev.1, November 2017

Article 10 of the European Convention on Human Rights stipulates the right to receive and impart information. Within its scope included are the methods in which the information is transmitted and received, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[252] "As a new and powerful information tool, the Internet falls undoubtedly within the scope of Article 10."[253]

Accordingly, the European Court of Human Rights has recognized the importance of the Internet and has also condemned the blocking of the Internet access.[254] The Court in *Times Newspapers Ltd v. the United Kingdom* stated: "In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10".[255]

Then, the Court in *Yıldırım v. Turkey* stated that blocking Internet access may be "in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured 'regardless of frontiers'".[256] There, a Turkish court blocked everyone's access to all *Google Sites*, the websites made by the users and hosted by Google. In a criminal proceeding against a third party's Google Site under a law prohibiting insults against the memory of Atatürk, all access to Google Sites was blocked, including the plaintiff's.

Although this blocking was done by an independent judiciary, the Court found a violation of Article 10 for the following reason (§§ 66-68): (1) failing to examine whether a method could have been chosen whereby only the offending Google Site was made inaccessible; (2) failing to take into consideration "*a significant collateral effect*" of rendering large quantities of information inaccessible to all Internet users; (3) not having domestic legal safeguards to ensure that a blocking order in respect of a specific site is not abused as a means of blocking access in general.

The Court emphasized that "the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest", rejecting Turkey's argument that Internet is only one of the means of accessing and imparting the information.

This is important because, in another ECtHR case *Akdeniz v. Turkey*,[257] the Court found no violation on a copyright blocking order on "*myspace.com*" and "*last.fm*", reasoning that "the users of those websites concerned were deprived of only one among many means of

---

[252] European Court of Human Rights, Internet: Case-law of European Court of Human Rights, Updated June 2015, Council of Europe, p. 44-46 (citing *Autronic AG v. Switzerland*, 22 May 1990, § 47, Series A no. 178; *De Haes and Gijsels v. Belgium*, 24 February 1997, § 48, *Reports of Judgments and Decisions* 1997-I; *News Verlags GmbH & Co.KG v. Austria*, no. 31457/96, § 39, ECHR 2000-I).

[253] European Court of Human Rights, Internet, supra, p. 44

[254] European Court of Human Rights, Internet, supra, p. 44-46

[255] *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, nos. 3002/03 and 23676/03, § 27, 10 March 2009 For background, see https://www.pinsentmasons.com/out-law/news/ceaseless-liability-for-internet-libel-is-not-a-barrier-to-free-speech-rules-echr

[256] *Ahmet Yıldırım v. Turkey*, no. 3111/10, ECHR 2012, § 67

[257] *Akdeniz v. Turkey* (dec.), no. 20877/10, ECHR 2014

listening to music and could easily access a whole range of musical works in many other ways without infringing copyright laws."

What is the difference when myspace.com and Google Sites? The Research Division of the European Court of Human Rights has the following to say on that matter:[258]

> State interference in the form of blocking or restricting access to the Internet is subject to strict scrutiny by the Court. Recent case-law shows that the extent of the States' obligations in the matter depends on the nature of the information posted online, the subject matter, and the status of the applicant (owner or user of a site). Where infringements of "*copyright protection*" are concerned which do not raise any important question of general interest, the Court considers that the domestic authorities enjoy a particularly wide margin of appreciation (*Akdeniz v. Turkey* (dec.), cited above, § 28). This also applies to users of commercial websites, but the margin of appreciation enjoyed by the States must be put in perspective when what is in issue is not a strictly "*commercial*" message but one that contributes to a debate on matters of "*general interest*" (*Ashby Donald and Others*, cited above, § 41). . .In such a case, in order to comply with Convention standards it is necessary to adopt a particularly strict legal framework - one that limits the restriction and provides an effective safeguard against possible abuse. In this case the blocking of Internet access produced a serious "*collateral censorship*" effect (*Ahmet Yıldırım*, cited above, §§ 64-66). In this case the Court acknowledged and upheld the "*rights of Internet users*" and the need for the national authorities - including the criminal courts - to weigh up the competing interests at stake. Any restrictions must be limited to what is strictly necessary to achieve the legitimate aim pursued.

However, please note that the UN Special Rapporteur La Rue diverges on this and will apply the same high standard to copyright-protective Internet blocking[259]even when it affects only a small number of people who have repeatedly infringed on copyright as in three strikes situations. The more operative difference seems to be the necessity, i.e., is it necessary to stop one from using all of the Internet when only parts of the person's activity is illegal.

Europe's relative leniency on website blocking is shown also through a CJEU case *Telekabel Wien GmbH v Constantin Film Verleih GmbH* ('Telekabel') where the court approved a website blocking order on an entire website for copyright violation, though, under the following condition: [260]

> [T]he measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services for lawful access. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.

It is difficult to imagine how not to affect lawful users when the entire website is blocked.

The UK case *Cartier Int'l AG v. British Sky Broadcasting* shows the difficult balancing between the intellectual property rights guaranteed by Article 17(2) and the

---

[258] European Court of Human Rights, Internet, supra, p. 46

[259] Frank La Rue, 2011 Internet report, Paras. 78-79

[260] *Telekabel Wien GmbH v Constantin Film Verleih GmbH*, C-314/12, ECHR (2014), para 55 and 56.

freedom of information of internet users under Article 11 of the EU Charter[261] on a trademark-related website blocking application: "(i) neither Article as such has precedence over the other; (ii) where the values under the two Articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or 'ultimate balancing test' - must be applied to each."

The lower court in *Cartier*[262] approved the blocking order under the following safeguards: (1) If there is a material change in circumstances, target websites and ISPs may apply to courts for a discharge of the blocking order; (2) The page shown to users who try to access blocked content must include details such as names of parties that obtained the order and inform users of their right to appeal such an order; and (3) When possible, such orders must carry a 'sunset' clause. The lesson from *Cartier* seems to be that we should acknowledge the impossibility of avoiding interference with lawful uses while blocking an entire platform and settle with a partial remedy of providing appeals process.

Then, in *Cengiz and Others v. Turkey*[263], concerning the wholesale blocking of access to *YouTube*, a website enabling users to send, view and share videos, for insulting Ataturk. The applicants, who were active users of the website, complained in particular of an infringement of their right to freedom to receive and impart information and ideas.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention, finding that the interference resulting from the application of the impugned provision of the law in question did not satisfy the requirement of lawfulness under the Convention and that the applicants had not enjoyed a sufficient degree of protection. The Court noted in particular that the applicants, all academics in different universities, had been prevented from accessing *YouTube* for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas. The Court also observed that *YouTube* was a single platform which enabled information of specific interest, particularly on political and social matters, to be broadcast and citizen journalism to emerge. The Court further found that there was no provision in the law allowing the domestic courts to impose a blanket blocking order on access to the Internet, and in the present case to *YouTube*, on account of one of its contents.

Turkey Domestic Courts

"Twitter.com" judgment: In March 2014, following several decisions in which the Turkish courts had found that Twitter was hosting content that was damaging to a person's private life and reputation, the TİB ordered the blocking of access to the site. In a judgment of 25 March 2014, the Ankara Administrative Court stayed the implementation of the TİB's order. In the meantime, on 24 and 25 March 2014, three individuals, including the second and third applicants, had applied to the Constitutional Court to challenge the blocking order.

In a judgment of 2 April 2014 (no. 2014/3986), the Constitutional Court held that the TİB's decision to block access to Twitter interfered with the right to freedom to receive and impart information and ideas. It noted, in particular, that delaying the posting of information or opinions shared via this medium, even for a short time, risked making the site devoid of all topical value and interest and that as a result the applicants, who were active users

---

[261] *Cartier Intl. v. Cartier Int'l AG v. British Sky Broadcasting*, [2016] WLR(D) 389.

[262] *Cartier Int'l AG v. British Sky Broadcasting* [2014] EWHC 3354 (Ch)

[263] *Cengiz and Others v. Turkey*, App. No. 48226/10, 14027/11, ECHR (2015)

of the site, had an interest in having the blocking order lifted promptly. Referring to the Court's judgment in *Ahmet Yıldırım* (cited above), it also held that the measure in issue had had no legal basis.

"YouTube" judgment: On 27 March 2014 the TİB issued an order blocking access to YouTube, particularly in the light of a judgment of the Gölbaşı Criminal Court of First Instance that certain contents hosted there violated state secrets and honor of Ataturk. In a judgment of 2 May 2014, the Ankara Administrative Court stayed the implementation of the TİB's order. Following the non-enforcement of that judgment, the YouTube company, the second and third applicants and six other individuals applied to the Constitutional Court.

In a judgment of 29 May 2014 (no. 2014/4705) , the court set aside the blocking order. Before addressing the merits of the case, it determined whether the applicants had the status of victims and held as follows.

> "27. ... It appears from the file that ... Yaman Akdeniz, Kerem Altıparmak and M.F. taught at different universities. These applicants explained that they carried out research in the field of human rights and shared the research via their YouTube accounts. They also stated that through the website they were able to access written and visual material from the United Nations and the Council of Europe ... The applicant, E.E., for his part, explained that he had a [YouTube] account, that he regularly followed users who shared files, as well as the activities of non-governmental organisations and professional bodies, and that he also wrote critical comments about the shared content ...
>
> 28. In the light of those explanations, it can be concluded that the applicants were direct victims of the administrative decision ordering the blocking of all access to www.youtube.com ..."

As to the merits of the case, with reference to *Ahmet Yıldırım* (cited above), the Constitutional Court found that the measure in issue had had no legal basis, particularly in the light of Law no. 5651, which did not authorise the wholesale blocking of an Internet site. It held as follows.

> "52. In modern democracies, the Internet has acquired significant importance in terms of the exercise of fundamental rights and freedoms, especially the freedom of expression. Social media constitute a transparent platform ... affording individuals the opportunity to participate in creating, publishing and interpreting media content. Social-media platforms are thus indispensable tools for the exercise of the right to freedom to express, share and impart information and ideas. Accordingly, the State and its administrative authorities must display considerable sensitivity not only when regulating this area but also in their practice, since these platforms have become one of the most effective and widespread means of both imparting ideas and receiving information."

Americas

The American Convention on Human Rights states in Article 13 that "Everyone has the right to freedom of thought and expression." and in paragraph 4 bans "prior censorship" except for the purpose of "protection of children".
The OAS Declaration of Principles on Freedom of Expression adopted 13 principles for the protection of freedom of expression. It recognizes in Principle 5 that "prior censorship, direct

or indirect interference in or pressure exerted upon any expression, opinion or information transmitted through any means. . . must be prohibited by law."[264]

The Inter-American Commission on Human Rights (IACHR)' Special Rapporteur of Freedom of Expression seems to agree with the United Nations' overall approach[265], rather than the European standard: restrictions on the rights to freedom of expression and access to knowledge on the Internet in connection to copyright protection must comply with the requirements established in the American Convention.[266] To wit, these limitations must pass the same three-prong test: (1) formal and material legality and legitimate objective; (2) necessity in a democratic society and; (3) proportionality. Moreover, there must be sufficient judicial control over the restriction in all cases with respect to due process guarantees, including user notifications.[267]

As a result, IACHR's Special Rapporteur specifically states that punishing users for violating copyright by disconnecting them is a disproportionate and radical measure that is not compatible with international human rights law, even when a gradual mechanism is employed (three strikes, for example, in which the Internet is disconnected after three violations).[268] Also, the measure should be "subjected to a strict balance of proportionality and be carefully designed and clearly limited so as to not affect legitimate speech that deserves protection."[269] Blocking is exceptional and should be applied only to illegal content,[270] which makes any form of Internet shutdown, website blocking or any other non-content-based (as opposed to forum-based) remedies illegitimate under the Convention.

IACHR Special Rapporteur's stern approach seems to rely on the belief that website blocking constitutes "prior censorship."[271] No matter how proportionate and necessary the limitations on freedom of speech are, they should not be applied through prior censorship and can only be prosecuted after the dissemination of the information through the subsequent and proportional imposition of liability.[272] To specific, removal of specific links is considered prior censorship.[273] Removing a link prevents all contents on the web page destined by that link from being accessed by anyone, and therefore constitutes prior censorship on those contents. Now, removing a link is in effect equivalent to blocking a website terminated by that link. Therefore, website blocking constitutes prior censorship.

The Inter-American Court of Human Rights, although lacking any case law directly on website blocking, is likely to support IACHR Special Rapporteur's position given that the

---

[264] OAS Declaration of Principles on Freedom of Expression, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26 [https://perma.cc/G7HA-8NKX].

[265] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression. Standards for a Free, Open, and Inclusive Internet., March 15, 2017, Paragraphs 155-159

[266] IACHR, Annual Report 2013. Report of the Special Rapporteur for Freedom of Expression 2013 Chapter IV (Freedom of Expression and the Internet). OEA/Ser.L/V/II.149. Doc. 50. December 31, 2013. Para. 76.

[267] Id., Para. 55

[268] Id., Para. 81

[269] Id., Para. 85

[270] Id. Para. 86

[271] IACHR, The Inter-American Legal Framework regarding the Right to Freedom of Expression, OAS, Office of the Special Rapporteur for Freedom of Expression (2010) (Catalina Botero Marino)

[272] Id., para. 91.

[273] Id., para. 148

Court has stated "Article 13(4) of the Convention establishes an exception to prior censorship, since it allows it in the case of . . . moral protection of children . . . . In all other cases, any preventative measure implies the impairment of freedom of thought and expression."[274]

Overall, the Inter-American Commission does not seem to accept website blocking or Internet shutdown as consistent with the Inter-American Convention of Human Rights in any circumstances, a position stronger than that of the European judiciaries.[275]

Brazil Domestic Courts

Brazil is unique in that social media blockings have originated from the judiciary that wanted to punish overseas social media platforms for not complying with court orders either demanding user data or content takedowns.[276]

Most famously, *WhatsApp* was shut down 3 different times for not fulfilling data access orders that the judiciary have issued for criminal investigation purposes. The information sought for, if existing at all, was stored on servers outside Brazil. WhatsApp Inc. refused to execute the orders arguing that it was a foreign company operating in the U.S. and therefore that it was not under obligation to comply with direct requests for user data made by Brazilian judges under Brazilian Law and insisted that authorities had to resort to the process under mutual legal aid treaties (MLATs).

Three courts then ordered the ISPs to block Whatsapp.[277] The provisions authorizing such order are not clear. Some judges made explicit reference to art. 12, III of the Marco Civil da Internet, which provides for "temporary suspension" as a sanction to application providers for violations of art. 10 and art. 11, to justify the blocking orders. However, Art. 10 and art. 11 concern the ISPs' and app providers' obligations to protect privacy. The underlying investigations were not for any privacy violations taking place on Whatsapp but for child abuse, drug trafficking, and organized crime.

At any rate, it seems that the higher courts still accepted art. 12 of Marco Civil da Internet as a legitimate legal basis for the blocking but blocking orders were reversed by appellate courts, because of their "disproportionality."[278]

---

[274] I/A Court H.R., Case of "The Last Temptation of Christ" (Olmedo-Bustos et al.) v. Chile. Merits, Reparations and Costs. Judgment of February 5, 2001. Series C No. 73. para. 70.

[275] Subhajit Banerji, Savni Dutt, Ella Hallwass, Yindee Limpives, Miguel Morachimo, Mirena Taskova, Shelli Gimelstein & Shane Seppinni, The "Right to Be Forgotten" and Blocking Orders under the American Convention: Emerging Issues in Intermediary Liability and Human Rights, Intermediary Liability & Human Rights Policy Practicum, September 2017 (advised by Daphne Keller & Luiz Fernando Marrey Moncau), page 65

[276] de Souza Abreu, J. (2018). Disrupting the disruptive: making sense of app blocking in Brazil. *Internet Policy Review*, *7*(3). DOI: 10.14763/2018.3.928

[277] Justiça Estadual do Rio de Janeiro. (2016, July 17). Inquérito Policial 062-00164/2016, 2a Vara Criminal de Duque de Caxias, judge Daniela Barbosa Assumpção de Souza, July 17, 2016; Justiça Estadual de São Paulo. (2016, December 6). Processo de Interceptação Telefônica n. 0017520- 08.2015.8.26.0564, 1a Vara Criminal de São Bernardo do Campo, judge Sandra Regina Nostre Marques; Justiça Estadual de Sergipe (2016, April 26). Processo n. 201655090143, Vara Criminal da Comarca de Lagarto, judge Marcel Maia Montalvão

[278] Tribunal de Justiça do Piauí. (2015, February 26). Mandado de Segurança n. 2015.0001.001592-4, rapporteur Desembargador Raimundo Nonato Costa Alencar ; Tribunal de Justiça de São Paulo. (2015, December 17). Mandado de Segurança n. 2271462-77.2015.8.26.0000, rapporteur Xavier de Souza ; Tribunal de Justiça de Sergipe (2016, May 3). Mandado de Segurança n. 201600110899, rapporteur Ricardo Múcio Santana de Abreu Lima.

The Federal Supreme Court also issued a preliminary decision in a constitutional challenge against the 2016 Duque de Caxias criminal court's blocking order.[279]

In granting the preliminary injunction, the president of the Federal Supreme Court reasoned as follows:[280]

> the Law 12,965/2014 (Marco Civil da Internet) [the law commandeered to justify the blocking order] provides that the discipline of internet use in Brazil has, as one of its principles, the "guarantee of freedom of expression, communication and manifestation of thought, under the Federal Constitution". In addition, this legal framework is concerned with "preserving the stability, security and functionality of the network."

Justice Lewandowski highlighted the importance of instant messaging even to subpoenas and court decisions and emphasized that the messaging application has more than one billion users worldwide, and that Brazil has the second largest number of users. He suspended what he saw as an act apparently not "reasonable and proportionate" which "would leave millions of Brazilians without this communication tool."[281]

In 2012 and 2016, there were also orders issued to ISPs to block Facebook for failing to take down posts violating local election laws but these orders were not carried out because Facebook took down the posts, facing the threat of the blocking.[282]

Africa

The fundamental right to freedom of information and expression enshrined under Article 9 of the African Charter on Human and Peoples' Rights (the African Charter). The African Commission on Human and People's Rights made a resolution in 2016 referring to the UN Human Rights Council's 2012 Resolution "[c]all[ing] on States Parties to respect and take legislative and other measures to guarantee, respect and protect citizen's right to freedom of information and expression through access to Internet services." [283]

Then in 2019, the African Commission on Human and Peoples' Rights issued a public statement "express[ing] concern on the continuing trend of internet shutdowns in Africa, including in Chad, Sudan, the Democratic Republic of Congo (DRC), Gabon and Zimbabwe" and explained that "internet and social media shutdowns violate the right to freedom of expression and access to information contrary to Article 9 of the African Charter on Human and Peoples' Rights."[284]

For the first time in Africa, the Zimbabwe High Court in *Zimbabwe Lawyers for Human Rights v. Minister of State in the President's Office* ruled in a provisional order in

---

[279] Supremo Tribunal Federal. (2016, July 17). Medida Cautelar na ADPF 403, justice Ricardo Lewandowski (order suspending ban on WhatsApp).

[280] Federal Supreme Court Homepage, Highlights, July 19, 2016 http://www2.stf.jus.br/portalStfInternacional/cms/destaquesClipping.php?sigla=portalStfDestaque_en_us&idConteudo=321207

[281] Id.

[282] de Souza Abreu, *supra*.

[283] Resolution ACHPR/Res.362 (LIX) 2016 on the Right to Freedom of Information and Expression on the Internet in Africa, adopted during the 59th Ordinary Session, held from 21 October to 04 November 2016

[284] Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa, January 29, 2019.

January 2019 that the government had no power to order the internet shutdown that coincided with widespread protests in January.[285] In the terse ruling not explicit on the reasons for it, Judge Owen Tagu ordered full internet access to be restored, though stating verbally that "it has become very clear that the minister had no authority to make that directive."[286] The application did include the constitutional argument under the Fundamental Human Rights and Freedom of the country's Constitution, to which the government responded:

> The information that was being circulated on the popular communication platforms such as Whats App, Skype, Twitter and Facebook had far reaching consequences to national peace and security as evidenced by the violence that was perpetrated. The platforms had become mediums of inciting violence to the general populace. Their use for business purposes was outweighed the threats of violence that was communicated. . . . The subject rights were being abused and infringed on the rights of others in a violent and abusive manner. Any disgruntlement by the affected citizens should have prompted them to seek dialogue with the government. . .[287]

Asia

There is no regional human rights body in Asia. However, India which has covered the lion's share of the world's shutdowns consecutively since the numbers were counted witnessed one of the most important legal developments in the shutdowns in Jammu and Kashimir designed to pacify the protests against the new citizenship laws.

In Anuradha Bhasin v UoI [WP(C) 1031/2019] and Gulam Nabi Azad v UoI [WP(C) 1164/2019], the Indian Supreme Court laid down the law on the issue of Internet as follows:

Firstly, the Court held that "t*he right to freedom of speech and expression under Article 19(1)(a), and the right to carry on any trade or business under 19(1)(g), using the medium of internet is constitutionally protected".* This declaration would entail that any curtailment of internet access have to be reasonable and within the boundaries laid down by Art. 19(2) and 19(6) of the Constitution.

Then, the Court ordered all the shutdown orders to be published, "a settled principle of law, and of natural justice", as it "affects lives, liberty and property of people".

Also, the Court required that every shutdown order be "reasoned" and "the necessity of the measure as well as the "unavoidable" circumstance necessitating such order. The Court held that suspending internet services indefinitely is impermissible although it refused to strike down the 5-month-long on-going shutdown in Kashimir. The Court allowed the government to prove that a shutdown can be 'preventive' as opposed to reactive to a danger but ruled that such danger should be in the nature of "Emergency". Further, the enabling law cannot be used to suppress expression of opinion. Any order should state material facts to enable judicial review. The Court further stressed that principles of proportionality should be used

---

[285] *Zimbabwe Lawyers for Human Rights v. Minister of State in the President's Office,* HC 265/19, Zimbabwe High Court Held at Harare, Jan 22, 2019. Available at http://www.veritaszim.net/node/3396 <last visited March 13, 2020>

[286] AFP, "Zimbabwe Protests: Court rules against internet shutdown", January 22, 2019, available at https://www.thesouthafrican.com/news/zimbabwe-news-internet-access-returns/

[287] Id., Opposing Affidavit of Abigail Tichareva, paras., 6.2-7.4, filed January 18, 2019.

and the least intrusive measure applied. The Court held that there shouldn't be repetitive use of the enabling law as well as it would amount to abuse of power.

Finally, the Court held that any curtailment of fundamental rights should be proportional and that the least restrictive measures should be resorted by the State. Although the state opposed selective access to internet services based on lack of technology, the Court held that if such a contention is accepted, then the Government would have a free pass to put a complete internet blockage every time and that such complete blocking/prohibition perpetually cannot be accepted. The Court further held that complete broad suspension of Telecom services, be it the Internet or otherwise, being a drastic measure, must be considered by the State only if 'necessary' and 'unavoidable' and that the State must assess the existence of an alternate less intrusive remedy.

However, the only relief granted was a direction given to the State review all orders suspending internet services forthwith. The positive aspect of the judgment, according to Software Freedom Law Center is that "*the Court has laid down the law on Internet shutdowns with emphasis on proportionality and reasonableness. The need to issue reasoned orders along with the mandate to make all orders public could result in reduction of arbitrary shutdowns. Removing the veil of secrecy from shutdowns itself could help in reducing the number of shutdowns.*"[288]

Joint Declarations of Special Rapporteurs on Freedom of Expression

The consensus that a requirement to block whole sites is disproportionate and not compatible with the protection of human rights online, for whatever reasons, was confirmed in the 2011 Joint Declaration on Freedom of Expression and Internet signed by freedom of expression special mandate holders of various human rights institutions: "mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse."[289]

The analogy to banning a newspaper or broadcaster is doctrinally important because such ban works prospectively to the future articles or shows to appear in that newspaper or broadcasting channel and therefore becomes "prior restraint",[290] which is most strictly scrutinized as the most evil suppression on free speech in all jurisdictions.

---

[288] SFLC, "Safeguards for shutdown, Limited relief for Kashimir", January 2020 https://sflc.in/sc-judgment-safeguards-shutdown-limited-relief-kashmir

[289] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the Internet. June 1, 2011. Point 3 a).

[290] Joint Declaration on Freedom of Expression and the Internet, supra., Point 3 b).

Given that site blocking can be easily circumvented[291], it is apt that the Special Rapporteurs direct "greater attention . . . .to developing alternative, tailored approaches. . for responding to illegal content" instead of shutting part or whole of the Internet.[292]

Procedural safeguards are ever more important when entire sites are blocked: "The State must at all times require products intended to facilitate filtration by end users to be accompanied by clear information intended to inform those users on how the filters work and the possible disadvantages should filtering turn out to be excessive."[293]

Since then, the Special Rapporteurs continued to issue joint statements in the same light as follows:

> 2014 joint declaration: "States should actively promote universal access to the Internet regardless of political, social, economic or cultural differences, including by respecting the principles of net neutrality and of the centrality of human rights to the development of the Internet."[294]
>
> 2015 joint declaration: "Filtering of content on the Internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law."[295]
>
> 2019 Joint declaration: "The exercise of freedom of expression requires a digital infrastructure that is robust, universal and regulated in a way that maintains it as a free, accessible and open space for all stakeholders. Over the coming years, States and other actors should:
>
> a. Recognise the right to access and use the Internet as a human right as an essential condition for the exercise of the right to freedom of expression.
> b. Protect freedom of expression in accordance with international human rights law in legislation that can have an impact on online content.
> c. Refrain from imposing Internet or telecommunications network disruptions and shutdowns."[296]

---

[291] Roy, Alpana and Marsoof, Althaf, "The Blocking Injunction: A Comparative and Critical Review of the EU, Singaporean and Australian Regimes" (June 29, 2016). (2016) 38(2) E.I.P.R. 9. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2802037

[292] Joint Declaration on Freedom of Expression and the Internet, supra., Point 3 c)

[293] Joint Declaration on Freedom of Expression and the Internet, supra., Point 3 c).

[294] Joint declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, presented at the UNESCO World Press Freedom Day event, May 6 2014.

[295] Joint declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, presented at the UNESCO World Press Freedom Day event, May 4 2015.

[296] Joint Declaration on Challenges to Freedom of Expression in the Next Decade

IV. Recommendations

1. Minimum Legal Requirements

Given the absolute languages used by international human rights bodies and regional and domestic courts, shutting down the entire Internet in any region is a clearly excessive measure -- even if it is done for innocuous purposes of preventing cheating at examinations -- since it shuts down the full variety of communications enabled by the Internet that are not related to the purpose of the shutdown, and is therefore deemed a violation of human rights.

Likewise, blocking an entire social media platform also can never be a measure proportionate to the purpose desired. Blocking of a social media platform, the topic of this research effort, is especially more disproportionate than blocking of an ordinary website since the social media platform has much more diversity of authors and contents that are not related to the purpose of the blocking. The only exception, out of Europe, is blocking of a special purpose platform such as music sharing executed for the purpose of protecting intellectual property rights but it may not be an exception after all because the breadth of communications on the music-only platform is not so wide as to make its blocking automatically excessive.

Even when social media platforms are shut down to respond to the fake news causing hate crimes against minorities, research indicates that shutdown only makes the situation more volatile[297] and takes away information that can save lives.[298] As AccessNow states, "Whether they are justified as a measure to fight "fake news" and hate speech or to stop cheating during exams, the facts remain the same: internet shutdowns violate human rights."[299]

Furthermore, as pointed out by European and American human rights bodies, Internet shutdown or social media platform works as a "prior censorship" as to the contents that have not yet appeared online or on that blocked website. The prior censorship argument has been effective in invalidating shutdowns and blockings in major court cases.

2. Best Practices

Condemning the practices as infringing is relatively easy compared to crafting model laws that prevent them. As said before, the network operators or Internet Service Providers (ISPs) are almost always under the licensing by the state because the physical layer upon which Internet is provided consists of mobile telephony, local cable TV network or fiber network all operated under license. Wireless carriers require exclusive bandwidth licenses lest air waves do not interfere with one another and wired carriers require easement through underground conduits and on public electric poles through which broadband lines are

---

Declaration by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information. July 10, 2019

[297] Rydzak, J. "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." Available at SSRN: https://ssrn.com/ abstract=3330413

[298] KeepItOn 2018, page 6

[299] KeepItOn 2018, page 2

installed whether they are coaxial cable, optical fiber or telephone lines. In exchange of these licenses on public properties, ISPs are imposed heavy regulatory frameworks under which they owe public interest obligations. The laws are intentionally broadly worded as 'national security', 'combating illegal material', 'public security', 'regulatory compliance', 'conditions of license' in order to ensure their compliance with a broad range of situations. Also, as the government is the putative guardian of public interest, whether ISPs cooperate with government requests often become important indicia of whether they uphold public interest.

Therefore, governments are easily tempted to use this easily accessible regulatory power to effect shutdowns and blockings. As seen in the above cases, many shutdowns and blockings are effected under the name of public security, public safety, license enforcement, crime prevention, warrant enforcement, etc. Indeed, "Armed with a hammer, it is tempting for governments to regard the internet as a nail."[300]

The challenge is how to craft a law that finds a balance between public need to control licensed entities and government's temptation for abuse. If the operator is truly in violation of regulation or license conditions or otherwise derelicts its public interest duties, the state should be able to take punitive measures against the operator without forcing it to take down the network.

In order to address such concern infrastructure-wise, as India's case shows, centralizing all shutdowns through one national process will be important otherwise regional and local governments will engage in 'precautionary measures' for reasons of parochial politics. Also, as China's case shows, ISPs must be either not owned by the state or must be otherwise independent from the state at least in form in order to prevent unexplained shutdowns from taking place without notice.

Also, the shutdown powers must be constrained explicitly by the statutes enabling the relevant regulatory authorities so that shutdown is ultimately not resorted to. For instance, as in Australian law and American law, the power to cancel ISP licenses is limited to non-payment of license fees and any other violation of license condition or regulatory noncompliance is subject to monetary or civil penalties. This way, access to Internet is preserved without sacrificing public control over ISPs.

Even when license is revoked, it should not lead to the stoppage of the services. This may mean that public "take-over" may be necessary to continue the services. Also, the state should never be allowed to order shutdown of multiple ISPs.

If for reasons unique to the region, the shutdown power is somehow not abolished, it is important that the regulatory structure is not abused for suppressing media freedom. For instance, license revocation should not be for the reason of servicing or failing to block certain content. The challenge here is that the governments are not very transparent about the reason for shutdowns. To address mismatch between actual reasons and announced reasons, it will be preeminently important to require judicial approval for any shutdown order as in Kazakhstan. Such requirement for the judiciary's involvement will naturally include appeal process.

---

300 Chatam House, "Asia's Internet Shutdowns Threaten the Right to Digital Access", 18 February 2020

Internet Society provides the following broader recommendations that should be no doubt informing the judiciary and administrative entities involved in the shutdown or blocking decisions[301]:

> Grounded in the principles of international human rights law, proportionality and necessity assessments should guide the actions of any policymaker entertaining the use of Internet shutdowns as a policy tool.
>
> Necessity means that any restriction of Internet access must be limited to measures which are strictly and demonstrably necessary to achieve a legitimate aim. It should be demonstrated that no other measure would achieve similar effects with more efficiency and less collateral damages.
>
> Necessity also implies an assessment of the proportionality of the measures. Any restriction of Internet access must also be proportional. A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons.

Social media blockings are, though often administered by ISPs, different from shutdowns in that they are actions directed at certain content populating the target platform. Justification is stronger for social media blockings than for shutdowns especially if the target content concerns criminal or otherwise illegal activities, which explains the high number of blocking-enabling laws using the same as justification for blocking. Probably, unlike shutdowns, the best practice for social media blockings we will settle for will have to include some authorization for blockings. However, as Turkey's administrative censorship system has shown, the need for judicial oversight is, doctrinally speaking, greater for social media blockings than for shutdowns because website operators are not under public interest obligations and will be therefore unduly penalized when blocked. Even now, the relatively high number of judicial blockings process compared to judicial shutdowns process reflects this.

As Brazil's case shows, the judiciary can be also overzealous especially when they have their own objectives (e.g., executing warrants) and should be restrained with a proper statutory provision prohibiting using blocking power in a retaliatory manner. This principle of prohibition on retaliatory blocking should be extended to a principle of prohibition on retaliatory shutdown.

Although various best practices were developed by several civil society organizations for ISPs to follow[302], it is important for our research to focus on the recommendations to the state actors. Global Network Initiative's recommendation[303] on governance on network disruptions proposes to "include ministries other than communication and interior in the dialogue; focus on ministries that deal with high social impact and growing use of

---

[301] Internet Society, Internet Shutdowns: An Internet Society Public Policy Briefing, December 2019.

[302] Disconnected: A Human Rights-Based Approach to Network Disruptions. Global Network Initiative. June 2018. https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network- Disruptions.pdf ; Article 19, "Getting Connected: Freedom of Expression, Telcos, and ISPs", June 2017

[303] Disconnected, Global Network Initiative, supra.

information technology (health, education, economy)" makes sense in that it is through these ministries the negative impact on the larger population that the shutdown or social media blockings will have on the society will be properly appreciated. Germany and South Africa involve multiple government agencies for any shutdown is administered.