Seattle Journal of Technology, Environmental & Innovation Law

Volume 13 | Issue 2 Article 6

5-6-2023

A New Right is the Wrong Tactic: Bring Legal Actions Against States for Internet Shutdowns Instead of Working Towards a Human Right to the Internet (Part 1)

Jay Conrad
jconrad@seattleu.edu

A New Right is the Wrong Tactic: Bring Legal Actions Against States for Internet Shutdowns Instead of Working Towards a Human Right to the Internet (Part 1)

Jay T. Conrad

ABSTRACT

This article is the first of a two-part series dealing with an increasingly prevalent threat to human rights: State-sanctioned Internet shutdowns. Part 1 details the current tactics and impacts of Internet shutdowns and which human rights are most likely to be violated by or during a shutdown. Part 2 will address the deficiencies of advocating for Internet access to be a recognized human right as means of combatting shutdowns. Despite the popularity of this proposed solution, the harms of Internet shutdowns are better addressed through traditional legal avenues, such as bringing claims against the sanctioning state.

Table of Contents: Part 1

INTRODUCTION……………………………………………..…………………2
BACKGROUND ON INTERNET SHUTDOWNS..………………………….…..5
I. INCREASES IN THE FREQUENCY AND INTENSITY OF STATE-SANCTIONED INTERNET SHUTDOWNS IS A MAJOR CAUSE OF CONCERN…………….……..6
II. WHAT IS AN INTERNET SHUTDOWN?...9
A. Where and When Internet Shutdowns Are Likely to Occur.............10
B. How an Internet Shutdown Works...12
1. Legal Mechanisms…………………………………………12
a. Why ISPs Comply with Shutdown Orders………………..…16
2. Technological Mechanisms………………………….……...17
a. Blocking Access to the Internet……………………………19
b. Digital Curfews……………………………………….20
c. Limiting Access to Parts of the Internet……….…………20
1) IP and Protocol-based Blocking……………….……21
2) Deep Packet Inspection-based Blocking………………...22
3) URL-based Blocking……………………….………23
4) Platform-based Blocking………………………….…23
5) DNS-based Blocking…………………………….24
6) Identity-based Internet Limitations ..……………………25
A) Takedown Orders……………………………....27
B) Issues Specific to "Shutting Down" Group…………29
d. Bandwidth Throttling……………………………………30
III. HUMAN RIGHTS VIOLATIONS THAT ARE MOST LIKELY TO RESULT FROM AN INTERNET SHUTDOWN…………………………………………………32
A. Freedom of Expression…………………………………….….35

B. Freedom of Assembly…………………………………………..………37
C. Right to Life……………………………………………………….....38
D. Economic, Social, and Cultural Rights………………………….40
1. The Economic Impact of Internet Shutdowns…………….….…..41
CONCLUSION……………………………………………………………43

INTRODUCTION

Early 1990s Internet lore focused almost exclusively on the technology's positive countercultural attributes. Now, thirty years into the Internet's evolution, this narrative still rings true. Despite the existential issues raised by Web 3.0, "cancel culture,"[1] lax digital privacy[2] (including problematic data mining practices[3] and surveillance capitalism[4]), and harmful predictive risk models,[5] the Internet still plays a pivotal role in democracy, government accountability, and the liberation of marginalized identities.[6] This is especially so in politically unstable and economically developing regions where the Internet is a vital part of an ecosystem of political dissent, citizen journalism, and near-live informational updates.[7] It is no surprise, then, that criticism-sensitive governments have developed tactics which quell online dissent through blocking, limiting, or disrupting access to the Internet. Collectively, these tactics are known as *Internet shutdowns*.

Internet shutdowns most often occur in politically unstable regions of the world, and in authoritarian or democratic States alike.[8] These shutdowns result in a wide array of harms, impacting everything

[1] Eleanor Cummins, *The Internet Gave Rise to 'Cancel Culture OCD,'* WIRED, Jan. 30 2022, https://www.wired.com/story/cancel-culture-ocd-politics-mental-health-activism/ [https://perma.cc/HU4P-TEUJ].
[2] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/EM6F-FJSA].
[3] Julia Carrie Wong, *The Cambridge Analytica Scandal Changed The World – But It Didn't Change Facebook*, THE GUARDIAN (Mar. 18, 2019), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook [https://perma.cc/P4YG-7HU4].
[4] See generally, Shoshana Zuboff*, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.
[5] Heidi Ledford, *Millions of Black People Affected by Racial Bias in Health-care Algorithm*s, NATURE (Oct. 24, 2019), https://www.nature.com/articles/d41586-019-03228-6 [https://perma.cc/6MCP-CQN3].
[6] Michael Rozynek, *Digital Adoption is Transforming Dissent…and Facilitating the Rise of the State*, ATELIER.NET (Feb. 4, 2021), https://atelier.net/insights/digital-adoption-is-transforming-dissent...-and-facilitating [https://perma.cc/K533-9XAX]; Access Now, *#KeepItOn for democracy: elections and internet shutdowns*, YOUTUBE (June 8, 2021), https://www.youtube.com/watch?v=MOOxf5c0HlQ&ab_channel=AccessNow [https://perma.cc/YB8L-SRDA] (hereinafter "Access Now Video").
[7] Rozynek, *supra* note 6; Access Now Video, *supra* note 6.
[8] Jan Rydzak, *Disconnected: A Human Rights-Based Approach to Network Disruptions*, 8, GLOBAL NETWORK INITIATIVE (2018), https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf [https://perma.cc/RQ65-PVMN].

from elections, to protests, to the economy – and, at their worst, Internet shutdowns are connected with large-scale government-led atrocities, such as mass killings of political dissenters.[9] Both the use of Internet shutdowns as a tactic and the intensity of the shutdowns implemented are on the rise.[10] This trend will continue so long as means of holding States accountable for harms caused or exacerbated by shutdowns remains undeveloped.[11]

The international human rights community's increased awareness of Internet shutdowns' profound and varied impact has resulted in serious discussions of Internet shutdowns' role in violating established human rights and whether a human right to Internet access should be recognized by supervisory bodies.[12] These conversations are encouraging, but largely academic: the two most popular proposed approaches to developing a means of accountability against shutdown-wielding States have been advocating for the recognition of Internet access as a human right[13] and the use of a human rights-based approach (HRBA) in crafting localized anti-shutdown programs and policies.[14] But neither of these approaches are likely to result in true accountability for shutdown-sanctioning governments. Instead, lawyers and activists within the human rights community should identify and bring Internet shutdown-based claims of rights violations to friendly and impact-minded supervisory bodies so that a precedent for accountability, penalization, and redress for Internet shutdown-based harms can be established.

Using this traditional approach to accountability is ideal for two reasons. First, there is a strategic benefit to leveraging the predictable, established legal precedents surrounding already recognized human rights, such as freedom of expression, in order to yield the desired results of sanctions against the offending states and remedies for the harmed populations. Second, this approach and the successes defined by it will lay the necessary legal groundwork for bringing similar technology-based claims for other technologies increasingly wielded harmfully by

[9] David Kaye, *Primer on Internet Shutdowns and the Law*, 12, ACCESS NOW (Nov. 2016), https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/AccessPart_I.docx [https://perma.cc/WFZ6-GQRZ].

[10] *#KeepItOn: Fighting Internet shutdowns around the world*, ACCESS NOW, https://www.accessnow.org/keepiton/ [https://perma.cc/JSB4-TENT] (last accessed Jan. 16, 2023).

[11] *Id.*

[12] Catherine Howell & Darrel M. West, *The Internet As a Human Right*, BROOKINGS.EDU (Nov. 7, 2016), https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/ [https://perma.cc/L44R-YJCP]; *It's time to recognize internet access as a human right,* WEB FOUNDATION (Oct. 28, 2020), https://webfoundation.org/2020/10/its-time-to-recognise-internet-access-as-a-human-right/ [https://perma.cc/E85D-DTTV].

[13] Howell & West, *supra* note 12; Hendrick Mildebrath, *Internet Access as a Fundamental Right: Exploring Aspects of Connectivity*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE (July 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696170/EPRS_STU(2021)696170_EN.pdf [https://perma.cc/9ACW-D7K8].

[14] *It's time to recognize internet access as a human right, supra* note 12; *The Human Rights-Based Approach*, UNITED NATIONS POPULATION FUND, https://www.unfpa.org/human-rights-based-approach [https://perma.cc/7AMS-HE4V] (last updated Nov. 24, 2014); see as an example Christian Borja-Vega & Eva Kloeve, *Why a Human Rights Based Approach to Water and Sanitation is Essential for the Poor*, THE WATER BLOG (Sept. 28, 2018), https://blogs.worldbank.org/water/why-human-rights-based-approach-water-and-sanitation-essential-poor [https://perma.cc/K7XM-LW2K].

authorities against their own populations, such as AI surveillance and drones.

This article is the first in a two-part series regarding this issue. It starts with defining what an Internet shutdown is, identifying when governments are most likely to mandate shutdowns, and the frequency at which shutdowns occur. It then details the various legal and technological methods leveraged to accomplish shutdowns. Finally, it analyzes which human rights are most likely to be violated as a result of a shutdown. The second installment in the series will address the viability of the human rights community's current two approaches in tackling Internet shutdowns—advocating for a human right to Internet access and implementing localized HRBA anti-shutdown policies—against a more classical approach of bringing human rights violations to supervisory bodies without the additional pretext of creating "a new human right."

BACKGROUND ON INTERNET SHUTDOWNS

Internet connectivity is increasingly recognized as a vital aspect of the modern human experience. It plays a significant role in our economy, interpersonal interactions, political systems, entertainment, and other aspects of our daily lives. As of the beginning of 2023, more than 64% of the world's total population, or approximately 5.16 billion users, access the Internet each month, with the average Internet user spending about seven hours online each day.[15] The Internet's importance only increases as it becomes more accessible: globally, the amount of new Internet users was growing annually at 4.8% in 2021, and though this has slowed to approximately 2% year-over-year in early 2023, rates of Internet adoption continue to be higher in developing economies.[16]

When Internet connectivity is disrupted and users are disconnected from this increasingly important resource—whether the result of an accident, natural disaster, or an intentional act—the wide-reaching effects of the outage cannot be understated. For example, Saipan and Tinian lost internet connectivity in 2015 when an earthquake cut the only fiber optic cable connecting the islands to the Internet. As a result, air traffic control was forced to ground flights, automated teller machines stopped dispensing currency, and the heavily relied upon tourist economy crashed with the loss of functioning digital hotel reservation systems.[17] Intentional Internet shutdowns can have similarly dire effects. A

[15] *Digital Around the World*, DATAREPORTAL, https://datareportal.com/global-digital-overview [https://perma.cc/GG83-MFAB] (last visited Nov. 24, 2021).

[16] *Id.*

[17] Todd Emerson Hutchins, *Safeguarding Civilian Internet Access During Armed Conflict Protecting Humanity's Most Important Resource in War*, 22 COLUM. SCI. & TECH. L. REV. 127 (2020); *see also* Steve Weintz, *Forget Nuclear Weapons, Cutting Undersea Cables Could Decisively End a War*, THE NATIONAL INTEREST, https://nationalinterest.org/blog/buzz/forget-nuclear-weapons-cutting-undersea-cables-could-decisively-end-war-108651 [https://perma.cc/E8RY-X9JX] (last visited Nov. 24, 2021).

governmental power that wields control over its own population by severing or limiting Internet connectivity, even at the risk of impacting that nation's economy, access to information, and national security, is a serious concern that cannot remain unaddressed.

I. INCREASES IN THE FREQUENCY AND INTENSITY OF STATE-SANCTIONED INTERNET SHUTDOWNS IS A MAJOR CAUSE OF CONCERN

Internet shutdowns are being leveraged by States against their populations with an increasing frequency and intensity.[18] The total amount of global State-sanctioned Internet shutdowns has risen dramatically in a short period of time.[19] In 2016, there were 75 known incidents of intentional Internet shutdowns.[20] By 2019, there were 213 incidents tracked (a 184% increase in that three year period).[21] Although in 2020 the total number of Internet shutdowns (at 159 incidents) decreased slightly for the first time since this phenomena began being tracked by human rights groups, shutdowns in 2020 were instated for longer periods of time and were more impactful on affected populations, especially in light of the ongoing COVID-19 pandemic.[22] This trend continued, with 182 shutdowns of increasing length and severity in 2021, the most recent year with complete, comprehensive data on shutdowns available at the time of this publishing.[23]

The severity of the 2020 and 2021 Internet shutdowns serve as key examples of the trend of elongated shutdowns and repeat offenders. Most notably, one single Internet shutdown incident in Myanmar, which was continuous from June 2019 through 2020, is currently considered the world's longest recorded shutdown[24] and continued through 2021 via a series of elongated shutdowns, some of which lasted for over two months at a time (the shutdowns have also increased in severity since the military

[18] James Vincent, *Internet Shutdowns by Governments Have 'Proliferated at a Truly Alarming Pace,'* THE VERGE (Sept. 1, 2021), https://www.theverge.com/2021/9/1/22649909/internet-sthudowns-government-freedom-speech-data-access-now-jigsaw [https://perma.cc/88LD-GSJU]; *#KeepItOn*, ACCESS NOW, https://www.accessnow.org/campaign/keepiton/.

[19] *The State of Internet Shutdowns Around the World: The 2018 #KeepItOn Report*, ACCESS NOW, July 2019, at 3, https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf [https://perma.cc/26YP-834Q]; *Shattered Dreams and Lost Opportunities: A Year in the Fight to #KeepItOn*, ACCESS NOW, Mar. 2021, at 2-3, https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf [https://perma.cc/GTV8-9SU4] (hereinafter "Shattered Dreams").

[20] *The State of Internet Shutdowns Around the World: supra* note 19; *Shattered Dreams, supra* note 19.

[21] *The State of Internet Shutdowns Around the World: supra* note 19; *Shattered Dreams, supra* note 19.

[22] *Shattered Dreams, supra* note 19.

[23] Marianne Díaz Hernández & Felicia Anthonio, *The Return of Digital Authoritarianism: Internet Shutdowns in 2021*, ACCESS NOW (May 24 2022), https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf [https://perma.cc/K7ZC-AVGM] (hereinafter "The Return of Digital Authoriarianism").

[24] *Shattered Dreams, supra* note 19.

coup in early 2021[25]). In Ethiopia, more than 100 million people faced national Internet blackouts lasting more than two weeks at the peak of the COVID-19 pandemic in 2020, when access to critical Internet-based health information quite literally could mean life or death.[26] Associated with changes in the political regime and allegations of ethnic cleansing, the Ethiopian shutdowns remained in place for over two years, with people in the Tigray region only now able to access mobile Internet after a ceasefire was signed in November 2022.[27] Throttling to block access to social media was seen throughout 2020 and 2021: in 2020, the Vietnamese government throttled (slowed) access to Facebook until the social media platform succumbed to governmental take down orders, a tactic imitated by Russia in 2021 with Twitter, while in Jordan, Facebook live was throttled to block protest stream sharing.[28] Protests in Jammu and Kashmir also faced shutdown orders issued by the Indian administration approximately every two weeks throughout 2020 and 2021 in its attempt to quell protests, again impacting access to vital public health information related to COVID-19.[29] India accounted for a whopping 109 of 2020's 155 incidents and 106 of the 182 shutdowns in 2021, highlighting how a government, once it establishes a routine of responding to its concerns through Internet shutdowns, may be more likely to implement shutdowns regularly and without recourse.[30] (India's status as an outlier in the number of shutdowns implemented annually has been a notable trend since 2017, when renowned global Internet shutdown watchdog Access Now first began publishing data about shutdowns. To demonstrate the extremity of the amount of shutdowns in India, the next nearest contender in 2021 was Myanmar with 15 shutdowns.[31]) These select examples serve only as a partial representation of the expansive, dangerous, and often chaotic implementation of Internet shutdowns by governments against their own populations in 2020.

[25] Andrea Januta & Minami Funakoshi, *Myanmar's Internet Suppression*, REUTERS (April 7, 2021), https://graphics.reuters.com/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/ [https://perma.cc/8HWE-89YV]; *The Return of Digital Authoritarianism, supra* note 23, at 3.

[26] *Shattered Dreams, supra* note 19, at 3.

[27] *Shattered Dreams, supra* note 19, at 5; *Freedom on the Net 2021 Ethiopia*, FREEDOM HOUSE, https://freedomhouse.org/country/ethiopia/freedom-net/2021 [https://perma.cc/5BN4-QG5Q]; *The Return of Digital Authoritarianism, supra* note 23, at 2-3; Mukul Sharma, *Ethiopia's Tigray Had Longest-ever Period of Internet Shutdown,* WIO NEWS (Mar. 1, 2023), https://www.wionews.com/technology/ethiopias-tigray-had-longest-ever-period-of-internet-shutdown-in-2022-566941 [https://perma.cc/ES9C-LMHS].

[28] *Shattered Dreams, supra* note 19, at 5; *The Return of Digital Authoritarianism, supra* note 27, at 10, 16.

[29] *Shattered Dreams, supra* note 19, at 4, 16; *The Return of Digital Authoritarianism, supra* note 27, at 2, 4.

[30] *Shattered Dreams, supra* note 19, at 4; *The Return of Digital Authoritarianism, supra* note 27, at 4.

[31] Tinuola Dada & Peter Micek, *Launching STOP: the #KeepItOn Internet Shutdown Tracker*, ACCESS NOW (Sept. 7, 2017), https://www.accessnow.org/keepiton-shutdown-tracker/ [https://perma.cc/9FMG-CS7E] (last updated Nov. 16, 2017).

Of additional concern is that each year, new countries implement Internet shutdowns.[32] In 2019, eight new countries implemented shutdowns.[33] In 2020, two countries instigated their first government-backed Internet shutdowns: Cuba (blocking social media platforms) and Tanzania (disruption and throttling during elections), with the year peaking at twenty-nine countries in total implementing government-backed shutdowns during that year.[34] That total rose to thirty-four countries using shutdowns against their populations in 2021.[35]

To best understand the dire impacts that State-sanctioned Internet shutdowns can have on their populations, it must first be understood what an Internet shutdown looks like in practice, how an Internet shutdown works legally and technologically, and what types of human rights obligations could be violated by the intentional restriction of Internet access.

II. WHAT IS AN INTERNET SHUTDOWN?

An Internet shutdown, sometimes called a "network disruption," occurs when an institution restricts a specific population or region from accessing the Internet.[36] In practice, the institution is typically a government.[37] Internet shutdowns occur under both authoritarian and democratic governments.[38] An Internet shutdown can restrict Internet access for an entire state or territory, or it can restrict access for specific sub-regions within those borders.[39] Invariably, Internet shutdowns restrict a population's ability to communicate with each other and with the outside world.[40] An Internet shutdown might involve a complete disruption of a population's ability to connect with the Internet at large, or it might involve restricting access to particular websites or social media platforms.[41] Rendering the Internet unusable by slowing down connectivity speeds so that videos, media, or websites will not load, even if Internet access is not completely severed, is also classified as an Internet shutdown.[42]

[32] *Shattered Dreams, supra* note 19; Berhan Taye, *Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019*, ACCESS NOW, Feb. 2020, at 1, https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf [https://perma.cc/FZ3V-C38P] (last visited Mar. 8, 2023) (hereinafter "Targeted, Cut Off, and Left in the Dark").

[33] *Targeted, Cut Off, and Left in the Dark, supra* note 32, at 1.

[34] *Shattered Dreams, supra* note 19, at 19.

[35] *The Return of Digital Authoritarianism, supra* note 23.

[36] *Everything You Need to Know About Internet Shutdowns*, AMNESTY INTERNATIONAL (Feb 2, 2021), https://www.amnesty.org.au/everything-you-need-to-know-about-internet-shutdowns/ [https://perma.cc/34N8-PQ57].

[37] *Id.*

[38] Rydzak, *supra* note 8, at 8.

[39] *Everything You Need to Know About Internet Shutdowns*, *supra* note 36.

[40] *Id.*

[41] *Id.*

[42] *Id.*

Distinguishable from technical failures, intentional network disruptions can be either preventative or reactive; that is, government-mandated Internet shutdowns are typically either a reaction to a perceived real or potential threat or, increasingly, are used by governments preemptively against such threats.[43] The most common objective of an Internet shutdown is to restrict or slow the flow of information available through digital channels, including social media platforms, dedicated digital communication tools (such as WhatsApp or Voice over Internet Protocol [VOIP] services), or mobile communication.[44] This objective is even more prevalent when digital communication networks are fueling public dissent or protests against the government.[45]

A. Where and When Internet Shutdowns Are Likely to Occur

Geographically, Internet shutdowns are currently occurring regularly in India, Africa, the Middle East, and the Asia Pacific region.[46] Latin America, the Caribbean, and Europe have significantly less shutdowns occurring on a regular basis.[47]

Although this article will focus on State-mandated Internet shutdowns, it should be understood that a variety of institutions within a given region may initiate an Internet shutdown, and for a variety of reasons; that is, shutdowns are not exclusive to governments. Thus, which type of institution mandating the shutdown can be the primary indicator of where or when a shutdown is likely to occur. Consider, for instance, the growing trend of professional and academic institutions mandating Internet shutdowns on campus in order to reduce cheating.[48] For obvious reasons, this type of shutdown is most likely to occur during an exam period and to be localized to the academic environment.[49] Temporary mass public events may also cause an institution to initiate a shutdown (for example, wrestling matches [in India], visits by public figures [in India and the Philippines], and beauty contests [the Philippines] have all been cited as reasons for Internet shutdowns to occur).[50] These shutdowns are usually localized and limited to a window of time during which the event occurs, and can be initiated by a myriad of institution types, be it a university, corporation, entertainment outlet, or governmental branch, and noting that there can be significant overlap in some regions between types of institutions (for example, government-controlled media conglomerates). [51]

[43] Rydzak, *supra* note 8, at 6, 8.
[44] Rydzak, *supra* note 8, at 6.
[45] *Id.*
[46] *Shattered Dreams, supra* note 19, at 2.
[47] *Id.*
[48] Rydzak, *supra* note 8, at 8.
[49] *Id.*
[50] *Id.*
[51] *Id.*

The vast majority of Internet shutdowns, however, are mandated by governmental authorities and occur during times of political tension, upheaval, unrest, or uncertainty.[52] Government-promulgated shutdowns are most likely to occur when there is either an active threat or when there is an activity occurring (or likely to occur) which the government perceives as a potential threat.[53] For example, governments might use shutdowns as a national security measure after a terrorist attack as means to limit false information spread.[54] Or, a government might initiate a localized shutdown as a preemptive safety measure for a specific types of mass public event, such as a religious procession, that has been targeted historically with Internet-enabled IEDs and other terrorist technologies.[55]

Yet it would be disingenuous to imply that governments do not most commonly restrict digital communications access during times of unrest which are most threatening to themselves as institutions. Shutting down the Internet during or in anticipation of mass protest accounts for the majority of government-mandated network disruptions.[56] Internet shutdowns most often occur when political unrest is already known to be happening, but are also likely to occur during times of uncertainty which could potentially lead to unrest or mass protest, such as during contentious elections (as in Africa and Cuba, for example) or when unchecked political rumors are spreading (as in India and Pakistan).[57] Shutdown-sanctioning governments can and often do localize Internet shutdowns to areas where and when a protest is occurring or expected to occur, but nation-wide disruptions also continue to occur at an alarming rate and are most likely to occur when opposition to the government is vocal throughout the entire country.[58]

B. How an Internet Shutdown Works

There are two elements that contribute to governments' ability to disrupt digital communication through limited Internet access: legal mechanisms which grant governments legitimacy in their Internet-limiting actions, and technological mechanisms which make the actual limitations possible.

1. Legal Mechanisms

A government's ability to censor Internet-based content or restrict Internet access depends on its ability to exercise control over

[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*

telecommunication companies.[59] Governments restrict Internet access by ordering Internet Service Providers (ISPs) to limit subscribers' access.[60] The ISPs then carry out these orders on behalf of the government.[61] Governments have commonly had the authority to order these actions through legal means.[62] In 2016, a study found that more than half of the forty-four countries researched had laws that allowed the possibility of a government-mandated Internet shutdown.[63] This sample suggested to experts in the field that most countries have some law or regulation already in place which could be used to shut down networks.[64] Some countries, including the United States, have explicitly granted the government the authority to seize private telecommunication facilities, when necessary. [65]

As governments have come to recognize the powerful role that the Internet plays in modern acts of political dissent, an increasing number of laws and regulations have been passed which allow more government authority over the Internet, whether in the form of legitimizing shutdowns or severe censorship of Internet-based content.[66] Increasing numbers of governments have relied on outdated laws, laws with overbroad definitions, and local laws which lack transparency to legitimize their shutdown efforts.[67]

Governments can justify Internet shutdowns with telecommunications laws passed or updated years – and sometimes decades – before the Internet's impact was understood.[68] In some instances, these laws are from before the Internet was even developed.[69] For example, the Indian government has used a law enacted in 1885 and intended to regulate telegraphs to justify governmental take-overs of ISP networks, or, when seeking even broader power, it has relied on an even older colonial-era legal authority (the Code of Criminal Procedure) to

[59] Christopher Giles & Peter Mwai, *Africa Internet: Where and How Are Governments Blocking It?*, BBC NEWS (Jan. 14, 2021) (last visited Nov. 25, 2021), https://www.bbc.com/news/world-africa-47734843 [https://perma.cc/R7KF-J6FN].

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] Deniz Duru Aydin, *The Laws that Let the Internet Shutdowns Happen*, ACCESS NOW (May 25, 2016), https://www.accessnow.org/laws-let-internet-shutdowns-happen/ [https://perma.cc/Q5D5-WBA7]. For a detailed analysis of the shutdown laws, see the spreadsheet "*Analysis of shutdown laws"* (May 2016) available at https://www.accessnow.org/analysis-of-shutdown-laws.

[64] Kaye, *supra* note 9, at 9-10.

[65] Kaye, *supra* note 9, at 9-10; *EPIC v. DHS – SOP 303*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/documents/epic-v-dhs-sop-303/. [https://perma.cc/RV9D-CXW7] (last visited on Nov. 25, 2021).

[66] *See Thailand Empowers State Authorities to Violate Rights by Censoring Online Content,* ACCESS NOW (Aug. 10, 2021), https://www.accessnow.org/thailand-online-censorship/; see also *Turkey: Dangerous, Dystopian New Legal Amendments: New Censorship Threat with Elections Looming*, HUMAN RIGHTS WATCH (Oct. 14, 2022), https://www.hrw.org/news/2022/10/14/turkey-dangerous-dystopian-new-legal-amendments [https://perma.cc/SXT8-ED2M].

[67] Kaye, *supra* note 9, at 9.

[68] *Id.*

[69] *Id.*

justify shutdowns in the Jammu and Kashmir region under "actions to uphold public order."[70]

Laws with overbroad definitions allow governments to abuse the laws to their liking.[71] Broad definitions of "national emergency" and "national security" are of particular concern.[72] The Indian Code of Criminal Procedure is able to be used modernly, for example, in part because of its exceedingly broad language.[73] It allows "collective punishment" and "criminalize[s] all forms of political interactions and mobilization…[as] terrorist related" and threats to national security.[74] Consider also the Telecommunications Framework Law of the Democratic Republic of Congo, which allows the government to ban the use of "telecommunication facilities, in full or part, for any period of time as it deems fit, in the interests of public security and national defence [*sic*], the public telecommunications service, or for any other reason." [75] This law has been leveraged in the Democratic Republic of Congo to legitimize cutting off Internet access.[76] Likewise, the Central African Republican and Ethiopian governments have both historically issued State of Emergency declarations to legally justify Internet shutdowns, and the Ugandan government has cited "safety and public order" as the basis for its shutdowns.[77] Outside of Africa, the Italian government decreed in 2013 that an ISP could be required to give control of its network to Italian intelligence agencies in the "interests of national security" while the U.S. Department of Homeland Security's Standard Operating Procedure 303 (SOP 303) codifies "a shutdown and restoration process for use by commercial and private wireless networks during national crises."[78] A 2011 Report from the White House further asserted the government's authority to control private communication systems in the United States during "times of war and other national emergencies," and, in 2012, the White House approved an Executive Order which grants DHS the authority to seize private facilities "when necessary."[79]

Broad legislative language allows loopholes that are further exploited where and when legal transparency is lax.[80] Some countries are plagued by chronic opacity regarding laws and legal processes in general, and in those countries Internet shutdowns are likely to occur without any reference to justifying laws at all (as seen in Ghana and Uganda).[81] But

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] Shakir Mir*, J&K Internet Shutdown Based on 'Dubious' Legal Framework: Report*, THE WIRE (Aug. 26, 2020), https://thewire.in/government/jammu-and-kashmir-internet-shutdown-jkccs [https://perma.cc/495L-6NY3].

[74] *Id.*

[75] Kaye, *supra* note 9.

[76] *Id.* at 9.

[77] *Id.* at 9-10.

[78] Kaye, *supra* note 9, at 9-10; *EPIC v. DHS – SOP 303*, *supra* note 65.

[79] *EPIC v. DHS – SOP 303*, *supra* note 70.

[80] Kaye, *supra* note 9, at 9-10.

[81] *Id.* at 10.

lack of transparency can take many forms, all of which embolden a government's ability to exercise control over telecommunications companies, and democratic regions may rely on opaque legal practices to obtain control over telecommunications. The Italian decree mentioned above was not passed as law, but instead as an ad hoc agreement between the Italian government and ISPs, meaning that the public was not formally informed of this secret bilateral agreement.[82] When the U.S.'s SOP 303 was approved in 2006, it was never released to the public.[83] The Electronic Privacy Information Center (EPIC) lost a multi-year legal battle against the Department of Homeland Security for it to reveal the full text of SOP 303 and the criteria used to determine if an Internet shutdown is necessary.[84] The lawsuit was instigated after an Internet shutdown occurred in San Francisco in 2011 to quell protests over a public transit officer's shooting and killing of a homeless man.[85]

a. Why ISPs Comply with Shutdown Orders

Why an ISP would comply with governmental shutdown orders to deny services to subscribers varies by country. In many places, such as throughout Africa and India, ISPs must obtain a license through the government in order to operate. This means that non-compliance with shutdown orders could result in a forfeiture of their operating licenses, loss of contracts, or fines.[86] Sometimes ISPs comply with shutdown orders due to risks of physical force or imprisonment by the government.[87] For example, in 2019, the Zimbabwean government ordered the country's largest telecommunications company to shut down all Internet services.[88] The Chairman of the company wrote on Facebook that the company "had to comply or management would face 'immediate imprisonment'" (this message was, of course, largely inaccessible to most people in the country at the time).[89] Finally, some ISPs are municipal. Because they are owned by public entities, complying with a shutdown order is an extension of the ISPs function as a government-run resource.

[82] *Id.*

[83] *EPIC v. DHS – SOP 303*, *supra* note 65.

[84] *EPIC v. DHS – SOP 303*, *supra* note 56*; see also* David Kravets, *Supreme Court Won't Force DHS to Reveal Secret Plan to Cut Cell Service*, ARS TECHNICA (Jan. 12, 2016), https://arstechnica.com/tech-policy/2016/01/supreme-court-wont-force-dhs-to-reveal-secret-plan-to-cut-cell-service/ [https://perma.cc/827J-JQFA] (last visited Nov. 25, 2021).

[85] *EPIC v. DHS – SOP 303*, *supra* note 65.

[86] Giles & Mwai, *supra* note 59. In the U.S., independent ISPs can legally operate without a license from the government, though they might have to comply with a court order to restrict services—though this would likely trigger a lengthy appeals process that outlives the "need" for the initial shutdown. The U.S. has more ISPs than anywhere else in the world (more than 7.000). For more information, please visit *https://en.wikipedia.org/wiki/Internet_in_the_United_States*.

[87] *Explained: How Do Internet Shutdowns Work?,* TRTWORLD (Feb. 16, 2021), https://www.trtworld.com/magazine/explained-how-do-internet-shutdowns-work-44212 [https://perma.cc/85PM-S46X].

[88] *Id.*

[89] *Id.*

Although ISPs may have the right to appeal to the courts against the government-issued shutdown order, this rarely occurs in practice.[90] In the rare instances where it has occurred, the governments' authority to limit Internet connectivity is usually upheld.[91] In the even rarer instances where the court rules against a shutdown order, governments may retaliate by passing new legislation allowing even greater governmental control over the Internet, as happened in Zimbabwe in 2019.[92]

2. Technological Mechanisms

The Internet is a network of networks.[93] When a user connects to an ISP via an Internet-enabled device, the device becomes part of the ISP's network.[94] The ISP may then connect to a larger network and act as a bridge between the user's device and other networks which host the content the user seeks to access through the device.[95] There is not an overall controlling network, but instead, merely multiple networks connected together though Network Access Points (NAPs).[96] NAPs are how networks connect together in order to exchange information between each other.[97] These network connections are what create the "Web," as the Internet is informally called; when many globally-based networks are webbed together, the "World Wide Web" is created.[98] Where local users can access the ISP's network through their devices is called a Point of Presence (POP).[99] When a local user uses their device to connect to an ISP's POP, they can access the networks that the ISP is connected to through its NAPs.[100]

Information must travel through the ISP in order to be accessible to the user.[101] For example, when a connected user types a website's URL into their device's browser, this query is processed by the ISP.[102] The ISP sends the request to its interconnected networks via its NAPs until it

[90] Giles & Mwai, *supra* note 59.
[91] Giles & Mwai, *supra* note 59; *see also* Karishma Mehrotra, *Suspension of the Internet: What the Rules Say, What the [Supreme Court] Underlined,* THE INDIAN EXPRESS (Jan, 17, 2020), https://indianexpress.com/article/explained/suspension-of-the-internet-what-the-rules-say-what-the-sc-underlined-6220361/ [https://perma.cc/TF9G-RK3F] (last visited Nov. 25, 2021); *see also EPIC v. DHS – SOP 303*, *supra* note 65.
[92] Giles & Mwai, *supra* note 59.
[93] Jeff Tyson, *How Internet Infrastructure Works*, HOW STUFF WORKS, https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/Howstuffworks.htm [https://perma.cc/JFQ8-BZVD] (last visited on Nov. 25, 2021).
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] Tyson, *supra* note 93.
[100] *Id.*
[101] *Explained: How Do Internet Shutdowns Work?, supra* note 87.
[102] A URL, or "Uniform Resource Locator," is simply the address of a given unique resource on the Web, often a webpage or website. *How Does the Internet Work: A Step-by-Step Pictorial*, HEWITT PACKARD (May 24, 2019), hp.com/us-en/shop/tech-takes/how-does-the-internet-work [https://perma.cc/N32Y-FFRR].

reaches the target server where the requested information (in this case, the website) is hosted.[103] When this information request from the ISP is received by the target server, it earns its name by "serving up" the packets of requested information.[104] These packets of information are then sent back through the network to the user's device, where the information can be assembled and then be accessed by the user; ergo, the user can now view and use the requested website on their device.[105]

Although large telecommunications companies do often have dedicated "backbones" (infrastructure such as fiber optic cables, modems, and other equipment necessary for network and service provision to function) where they offer service, "shutting off the internet" does not involve changes to the literal hardware that allows local access to the Internet.[106] Simply put, there is no Internet off-switch.[107] Instead, Internet access is controlled by limiting which networks, websites or apps local users can access when connected to the ISP.[108] Limiting users' Internet access may involve restricting access to POPs (no local access point to the Internet), restricting which NAPs users can access (creates a limited or "bordered" Internet), blocking users' ability to request information from certain servers or networks which are connected through the ISP's NAPs (makes certain sites, such as Twitter or Facebook, inaccessible to users), or by "throttling" or slowing the speed at which the packets of information are delivered to the user through the ISP (causes websites or information to simply not load due to slow information delivery speeds, making it nearly impossible for the device to reassemble the information requested such that the user can access it).[109] Each of these intentional Internet access limitations is a form of Internet shutdown.

The four most common types of intentional access limitation that are recognized as Internet shutdowns will now be detailed in the following order: 1) blocking access to the Internet outright; 2) use of digital curfews; 3) limiting access to some parts of the Internet, of which there are five common types; and 4) bandwidth throttling.

a. Blocking Access to the Internet

To block access to the Internet so that no local users can connect to it, governments can order ISPs to restrict network connectivity to the area

[103] *How Does the Internet Work, supra* note 107.

[104] *Id.*

[105] *Id.*

[106] Tyson, *supra* note 93; *Explained: How Do Internet Shutdowns Work?, supra* note 87.

[107] *Explained: How Do Internet Shutdowns Work?, supra* note 87.

[108] *How Does the Internet Work, supra* note 102.

[109] *Explained: How Do Internet Shutdowns Work?, supra* note 87; Gopal Sathe, *How ISPs Block Websites and Why It Doesn't Help*, MINT (Sept. 5, 2021), https://www.livemint.com/Politics/L8Yq3CxyG33nPQJMJilXRM/How-ISPs-block-websites-and-why-it-doesnt-help.html [https://perma.cc/EJS7-DP8N].

entirely.[110] All traffic (information sent through the network) can be blocked by the ISP if so ordered.[111] This results in there being "no Internet."[112] As mentioned before, there is no overall controlling Internet; thus, when the Internet is "shut down" in one region, other regions can still maintain access to the Internet.[113] The government determines whether the network disruption should be localized or nationwide and will specify such parameters in its order to the ISP. The ISP may execute the network disruption by restricting users' devices' access to POPs or NAPs, resulting in users' inability to send or receive information through the networks that the ISP is connected to. Reasons for the restrictions may be transparent; ISPs may choose to alert users that the network disruption is the result of a government order, as was done by an Iraqi ISP in 2018.[114] There, when users attempted to load apps or webpages, they would receive a message from the ISP stating that the government had ordered the Internet cut off.[115]

b. Digital Curfews

Governments may order Internet connectivity to be shut off at specific times while still allowing Internet use during "business hours."[116] This is called a "digital curfew."[117] From a technical standpoint, the ISP's execution of the shutdown order is the same: ISPs restrict users' access to the network by blocking their devices' connection to its NAPs and POPs, but only for specified windows of time.[118] Digital curfews are a way in which a government attempts to limit its populations from using the internet to do things such as organize protestations against it, but without crashing its Internet-reliant economy.[119]

c. Limiting Access to Parts of the Internet

A government might opt to limit a population's access to particular parts of the Internet rather than order a complete stoppage on regional Internet connectivity. This type of Internet shutdown allows users to continue to access the majority of the Internet while not being able to access specific information or websites that the government has deemed

[110] *Explained: How Do Internet Shutdowns Work?, supra* note 87; Wall Street Journal, *How Governments Shut Down the Internet*, YOUTUBE (Feb. 27, 2020), https://www.youtube.com/watch?v=53q3gscB7FM&ab_channel=WallStreetJournal [https://perma.cc/RNC6-MQ6B].
[111] *Explained: How Do Internet Shutdowns Work?, supra* note 87.
[112] *Id.*
[113] Tyson, *supra* note 93.
[114] Wall Street Journal, *supra* note 110.
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Explained: How Do Internet Shutdowns Work?, supra* note 87.
[119] Wall Street Journal, *supra* note 110.

problematic or threatening.[120] As a general principle, it is easy for ISPs to limit users' access to certain content as all content must pass through the ISP's infrastructure in order to reach the end user; ultimately, the ISPs have full control over which content or information is reaching users.[121]

There are five techniques commonly used to limit access to part of the Internet: IP and Protocol-based blocking, Deep Packet Inspection (DPI)-based blocking, URL-based blocking, Platform-based blocking, and Domain Name System (DNS)-based blocking.[122] Of these, URL-based blocking, DNS-based blocking, and DPI-based blocking are the most common ways of intentionally limiting Internet access.[123] Governments may also try to limit an individual's access to certain parts of the Internet, like social media platforms, if they have deemed that person a potential threat—a tactic based in politically and legally pressuring service-providing companies rather than using technological methods of Internet limitation.[124] Thus, this individualized approach can be an alternative to limiting Internet access more broadly for a region, locality, or portion of the population.

1) IP and Protocol-Based Blocking

IP and Protocol-based blocking is one of the simplest ways to deny access to information without directly blocking any specific content.[125] Instead of blocking the content itself, IP and Protocol-based blocking prevents all traffic to IP addresses which are associated with certain types of content, topics, or information.[126] While IP-based blocking may be a generally useful tactic for governments seeking to block all content from a specific app or a particular region of the world, its effectiveness can be undermined through easily-accessible and well-known techniques, like using a VPN.[127]

[120] *Internet Society Perspectives on Internet Content Blocking: An Overview*, INTERNET SOCIETY (March 24, 2017), https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/ [https://perma.cc/ALC8-WG3C].
[121] Sathe, *supra* note 109.
[122] *Internet Society Perspectives on Internet Content Blocking, supra* note 120; *Explained: How Do Internet Shutdowns Work?, supra* note 87.
[123] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.
[124] *Self-Regulation and 'hate speech' on social media platforms*, ARTICLE 19 (Mar. 2018), https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms_March2018.pdf [https://perma.cc/4L9Q-GXBL].
[125] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.
[126] *Id.*
[127] *Id.* A VPN is a "virtual private network" that creates an encrypted tunnel for Internet browsing such that the location of one's internet connection and data packets being exchanged while online are kept private. For more information, see *What is a VPN?*, NORDVPN, https://nordvpn.com/what-is-a-vpn/.

2) Deep Packet Inspection-Based Blocking

Deep Packet Inspection (DPI) is typically used for network security reasons.[128] DPI-based blocking allows for the filtering of specific content, patterns or application types.[129] The "packets" being inspected are the packets of information sent as responses by the query-receiving server, and which are sent through the NAPs to the end user's device.[130] DPI blocking allows some of these packets of information to reach the user's device, while packets of information containing restricted content are stopped from reaching the user.[131] When the packets are re-assembled on the device so that the user can access the information or website served to them, the restricted content is "filtered" out such that only non-restricted content is available to the user.[132]

DPI blocking requires signatures, keywords, or other content-specific information to be known and incorporated into "blocking rules" in order to be effective.[133] Although more computationally intensive than other blocking methods as all content passing through the NAPs must be evaluated against the blocking rules, DPI blocking can be effective against certain applications (such as VOIP traffic) or data file types (such as videos).[134] Since users under a DPI regime can continue accessing the Internet without a noticeable disruption in service overall, they might not realize that information or topics are being intentionally made inaccessible; DPI-blocking might make it appear that a site simply will not load because its security certificate is not trusted, or a specific piece of content, like an embedded video, might appear to be endlessly buffering and unplayable.[135]

3) URL-Based Blocking

URL-based blocking is one of the most popular types of blocking methods, although it only works for web-based applications.[136] Entire categories can be blocked using this technique because URLs are generally

[128] Chris Brook, *What is Deep Packet Inspection? How it Works, Use Cases for DPI, and More*, DIGITALGUARDIAN.COM (Dec. 5, 2018), https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more [https://perma.cc/CJ22-RUXE].

[129] *Id.*

[130] Tyson, *supra* note 93.

[131] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[132] *Id.*

[133] *Internet Society Perspectives on Internet Content Blocking, supra* note 120. Blocking rules are classifications set within a firewall (a network security system that establishes a barrier between networks) that determine the flow of information between networks. If certain information is "blocked" (stopped from entering the network) as a "rule" (whenever that classification is identified, it is always stopped), then the information will not be allowed into the network nor will it be accessible to a person using that network.

[134] *Id.*

[135] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[136] *Id.*

managed by category (such as "news sites").[137] A URL filter could simply stop traffic from accessing these categories of sites with no notice to the user of what has occurred, or an ISP may choose to redirect users to a webpage explaining that or why the traffic was blocked.[138] URL-based blocking is effective at identifying and blocking content because URLs do not change even when servers change IP addresses.[139]

4) Platform-Based Blocking

It is possible for ISPs to block some content from a platform without blocking the entire platform outright, but the platform owner has to assist the ISP in order for the effort to be successful.[140] This technique can be used to block certain search results, information, or content from appearing to the user as they are using the platform while still allowing the user to access the platform itself.[141] Usually, the platform in question is a major search engine (like Google) or major social media platform (like Facebook or Twitter).[142]

Looking specifically at search engine platform blocking, only "pointers" to information can be made inaccessible to the user rather than the content itself.[143] Search engine blocking is only mildly effective at making content inaccessible to users because the content is still available if the user is accessing it directly (without the assistance of the specific search engine) or accessing it through a different search engine that is not blocking the content.[144] Nonetheless, this technique remains popular with governments looking to limit access to the Internet within their jurisdiction and who petition platforms to apply filters to search results that comply with regulations, ethos, or the political needs of the regime.[145]

5) DNS-Based Blocking

The Domain Name System (DNS) connects IP addresses with their URLs; DNS is the "phone book" of the Internet, telling queries where to go to retrieve the information sought.[146] DNS-based blocking impedes easy user access to requested domains by either re-routing the user's query

[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Internet Society Perspectives on Internet Content Blocking, supra* note 120*; see generally* conversations regarding "the great firewall of China;" *for example* Alex Hern, *Google 'Working on Censored Search Engine' for China,* THE GUARDIAN (Aug. 2, 2018), https://www.theguardian.com/world/2018/aug/02/google-working-on-censored-search-engine-for-china [https://perma.cc/BKM6-QNKN] (last visited Apr. 2, 2023).
[146] *What is DNS? How DNS Works*, CLOUDFLARE, https://www.cloudflare.com/learning/dns/what-is-dns/ [https://perma.cc/8CMD-CLEV] (last visited Mar. 8, 2023).

to an alternative IP address or by claiming that the requested domain does not exist.[147] This is done through the use of a specialized server.[148] The special server is activated when the user queries a domain which appears on a "block list," per the rules that an ISP sets up in order to comply with a government-mandated shutdown order.[149] The effect is that the user is unable to access the website or any of its associated subdomains, and the ISP may serve up an alternative website instead via the specialized server.[150] If no alternative domain is served up to the user in response to the query, the user will be "told" by the ISP that the website and its sub-domains simply do not exist at all (a falsehood).[151]

6) Identity-Based Internet Limitations

The Internet limitation tactics discussed above have been used to shutdown Internet access geographically, whether that be defined as a country (Vietnam[152]), a sub-region of a state (the Jammu and Kashmir region of India[153]), a city (San Francisco[154]) or a micro-location (the Cox's Bazar Rohingya refugee camp[155]). From a technical standpoint, shutdown tactics are not deployed against specific identities, such as certain individuals or affinity groups. This is not to imply that governments do not implement Internet shutdowns with the specific intent of affecting particular identities, and in fact, this is commonly the case.[156] When a government attempts to limit Internet access for specific ethnic, political, or religious identities, for example, this can often be achieved geographically as many minority groups are geographically separated from other portions of the population.[157] Thus, regional Internet shutdowns often achieve the intended impact of primarily affecting certain identities.[158] Two examples of regional shutdowns targeted at minority groups are the Bangladesh government's Internet shutdowns in 2019 and 2020 targeting Rohingya refugee camps (geographically isolated religious minority),[159] and the Indonesian government's shutdowns tailored against Papua Indigenous groups (geographically isolated racial minority groups).[160] Yet regardless of a government's intentions, the ways Internet shutdowns are currently enacted do not technically target distinct identities; anyone who enters the shutdown zone, regardless of who they

[147] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Shattered Dreams, supra* note 19, at 5.

[153] *Id.* at 4, 16.

[154] *EPIC v. DHS – SOP 303*, *supra* note 65.

[155] *Targeted, Cut Off, and Left in the Dark, supra* note 32, at 11.

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] *Shattered Dreams, supra* note 19, at 12.

are, is equally affected by the Internet shutdown. That is, anyone entering the Rohingya refugee camp or Papua would have been affected by the Internet shutdown, not just the targeted identities therein.

Intentional governmental limitations on Internet access that go beyond the regional scope, especially the targeting of individuals, are not usually included in Internet shutdown statistics or studies. They are instead usually categorized as censorship rather than a shutdown.[161] However, identity-based Internet limitations have been included here because the ultimate effect of these State actions is the same as that of geography-based Internet shutdowns. What identity-first limiting techniques achieve is the limiting of access to certain Internet-based content, not just of the targeted identities but of the population at large. By silencing voices of dissent, the State is effectively—and often literally—removing individuals or groups from vital digital spaces used for organizing, disseminating information, and for keeping government actors accountable. The effect of this censorship is two-fold: it stops the individual or group from accessing some part of the Internet, and it also stops other users from accessing Internet-based content made by that individual or group. Furthermore, as digital surveillance technology continues to develop, it is reasonable to assume that in the near future governments will be able to target particular identities within a given region rather than implementing an Internet shutdown that affects all persons within a geography. With this future in mind, identity-specific Internet limitation tactics are included here.

A) Takedown Orders

To "shut down" an individual or group from free use of the Internet, governments can target key Internet profiles with takedown orders to the websites or platforms hosting the target's content. In issuing a takedown order, the government tells the hosting site or platform to disable the individual's profile or to make it inaccessible to other users of the platform.[162] Takedown orders do not require the ISP to remove the content on the government's behalf, making it distinct from most other shutdown tactics. It instead relies on government agents or agencies to lobby the content-hosting website or platform to remove the content.[163] The government's target is usually an influential voice of political dissent that is either involved in organizing protest actions or in citizen

[161] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[162] Alejandro Menjivar, *Waning: repressive Regimes are using DMCA Takedown Demands to Censor Activists,* ACCESS NOW (Oct. 22, 2020), https://www.accessnow.org/dmca-takedown-demands-censor-activists/ [https://perma.cc/2W5H-8YE5]; *see e.g.*, Karan Deep Singh & Paul Mozur, *As Outbreak Rages, India Orders Critical Social Media Posts to be Taken Down*, THE NEW YORK TIMES (May 27, 2021), https://www.nytimes.com/2021/04/25/business/india-covid19-twitter-facebook.html [https://perma.cc/SU5P-ZENP].

[163] Menijivar, *supra* note 162.

journalism.[164] Often, the government will claim that the individual's social media account should be "taken down" (deactivated) because it contains illegal content. When governments use takedown orders to limit Internet access for particular groups, the groups usually represent a political minority identity.[165]

Governments are increasingly aggressive in issuing and enforcing takedown orders.[166] Twitter saw a surge globally of governments demanding that the platform take down content in 2020.[167] The platform reported a 26% jump in the amount of takedown orders issued specifically against journalists and news outlets between the first half of 2020 to the second half.[168] Alarmingly, also in 2020, governments began retaliating against platforms that were not complying with takedown orders by employing other Internet shutdown methodologies in an attempt to force the platforms' compliance.[169] The Vietnamese government retaliated against Facebook by intentionally slowing the bandwidth of the platform (a tactic called throttling[170]) in retaliation against Facebook's initial refusal to comply with issued takedown orders.[171] Slowing a platform greatly affects a platform's use in the region and thus impacts the platform's revenue.[172] The Vietnamese government's throttling was meant to scare Facebook into compliance with its takedown orders by threatening its bottom line—and it worked.[173] Thailand retaliated against Twitter and Facebook by bringing criminal charges against the platform for its refusal to comply with issued shutdown orders.[174] The Thai government's digital minister demanded that the companies send representatives to negotiate in order to have the charges dropped and to avoid fines.[175] Digital freedom advocates say this is a tactic to scare the companies into compliance, though whether Thailand will be successful is yet to be seen.[176]

[164] *Id.*
[165] *Id.*
[166] Sheila Dang & Elizabeth Culliford, *Twitter Sees Jump in Gov't Demands to Remove Content of Reporters, News Outlets*, REUTERS (July 14, 2021), https://www.reuters.com/technology/exclusive-twitter-sees-jump-govt-demands-remove-content-journalists-news-outlets-2021-07-14/ [https://perma.cc/CHB8-FZNE]; Patpicha Tanakasempipat & Panarat Thepgumpanat, *Thailand Takes First Legal Action Against Facebook, Twitter Over Content*, REUTERS (Sept. 23, 2020), https://www.reuters.com/article/us-thailand-internet/thailand-takes-first-legal-action-against-facebook-twitter-over-content-idUSKCN26F0R7 [https://perma.cc/3743-F9A7].
[167] Dang & Culliford, *supra* note 166.
[168] *Id.*
[169] *Shattered Dreams, supra* note 19, at 5.
[170] Bandwidth throttling as a shutdown tactic will be discussed in the next section.
[171] *Shattered Dreams, supra* note 19, at 5.
[172] *Id.*
[173] *Id.*
[174] Tanakasempipat & Thepgumpanat, *supra* note 166.
[175] *Id.*
[176] *Id.*

B) Issues Specific to "Shutting Down" Groups

Groups may face unique issues or forms of oppression from governmental attempts to limit their identity's Internet access due to special dynamics that may exist in these groups. Consider how the Chilean government prohibited leaders of the Mapuche people, a politically active Indigenous community, from owning, directing, or managing any social media.[177] In this case, the Chilean government utilized its anti-terrorism legislation to limit the Internet access of the Mapuche movement leaders due to ongoing conflict regarding the Indigenous group's rights within Chilean territory.[178] The Chilean government intended to limit content from the Mapuche people from appearing online as a form of quelling dissent.[179] Although the government restricted individual leaders and not all Mapuche people from social media, the nature of the Mapuche social structure is that community leaders (*llongkos*) play an essential role in Mapuche society.[180] As traditional authorities of the Mapuche people at the time that the restrictions were implemented, the leaders held decisive roles in communicating the interests of the Mapuche with non-Mapuche authorities, as well as leading the political, spiritual, and social direction of their respective communities.[181] The effect of restricting the Internet use of Mapuche leaders was to limit the Internet access of the Mapuche community.[182] In addition to silencing Mapuche authority figures, the Internet restrictions levied against the leaders caused other Mapuche people to self-censor, including digitally, for a reasonable fear of prosecution by the Chilean government.[183] In 2014, the Inter-American Court of Human Rights held that the restrictions on the Mapuche leaders violated their right to freedom of expression and that the restrictions impacted the Mapuche community by deterring the community's exercising of freedom of expression.[184] The impact of the initial restrictions still linger and might explain why there is very little information available online about the Mapuche community, with the available information coming from non-Mapuche sources.

[177] *Norín Catrimán v. Chile*, Global Freedom of Expression, COLUMBIA UNIVERSITY https://globalfreedomofexpression.columbia.edu/cases/norin-catriman-v-chile/#:~:text=The%20Inter%2DAmerican%20Court%20of,freedom%20of%20thought%20and%20expression [https://perma.cc/N6AT-JAB9] (last visited Mar. 8, 2023).

[178] *Id.*

[179] *Id.*

[180] *Mapuche*, MINORITY RIGHTS, https://minorityrights.org/minorities/mapuche-2/ [https://perma.cc/TE9E-S6JH] (last visited Mar. 8, 2023).

[181] *Norín Catrimán v. Chile*, *supra* note 177.

[182] *Id.*

[183] This case will be discussed further in the second installment of this two-part series, in a section on "Limited Successes in the Courts." *Id.*

[184] *Id.*

d. Bandwidth Throttling

"Throttling" is distinct from other types of Internet shutdowns in that it does not outright restrict, limit, or block users from accessing content.[185] Throttling is when an ISP is ordered to deliberately slow the Internet connectivity speed of a region such that the Internet is made inaccessible to users despite there being no technological "block" of websites or content.[186] When Internet connectivity is slowed, websites, platforms, and apps appear to work. However, users are unable to access the content therein; the content or videos either will not load at all or appear very low-resolution as a result of the slowed connectivity.[187]

In addition to difficulties in accessing content, uploading content and livestreaming[188] are direly impacted by throttling due to their reliance on faster connectivity speeds for success. Throttling effectively blocks users from being able to live stream in particular because livestreaming requires fast, consistent Internet connectivity to keep video broadcasting steadily over the Internet in real-time.[189] Livestreaming is a primary and popular tool for holding government and state actors accountable; throttling is a common way that states attempt to disrupt this activist tactic.[190] In addition to effectively stopping the up or download of information, throttling may discourage users from using certain apps or services, causing users to think that certain apps or services are unreliable, or encouraging users to utilize other (likely government-approved) services.[191]

Throttling is becoming an increasingly common tactic used by governments in response to mass demonstrations and protests.[192] It requires less work by both the government and the ISP to implement than other types of Internet shutdowns in that it does not require the curating, creating, or maintaining of a block list, specialized server, or complex set

[185] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[186] *UNSR Report: Internet Shutdowns and Freedom of Association and Assembly*, INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW (July 1, 2021), https://www.icnl.org/post/news/unsr-foaa-clement-voule-issues-report-on-internet-shutdowns [https://perma.cc/TC3X-JGZP]; *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[187] Wall Street Journal, *supra* note 110.

[188] "Livestreaming" is when video is streamed directly over the Internet in real time, without first being recorded or stored; it is equivalent to a televised live broadcast. For more information, please visit: https://www.cloudflare.com/learning/video/what-is-live-streaming/ [https://perma.cc/F7X2-5VKG].

[189] Samuel Woodhams, *The Rise of Internet Throttling: A Hidden Threat to Media Development*, CENTER FOR INTERNATIONAL MEDIA ASSISTANCE (May 20, 2020), https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/ [https://perma.cc/WH3E-CTK9].

[190] Lexi Pandell, *How Livestreaming is Transforming Activism Around the World*, WIRED (Nov. 16, 2016), https://www.wired.com/2016/11/livestreaming-transforming-activism/ [https://perma.cc/8N9S-NB8J]; *Jordan's internet throttling to censor protestors must end*, ACCESS NOW (Mar. 19, 2021), https://www.accessnow.org/jordan-protest-throttling/ [https://perma.cc/7FD8-YNGA].

[191] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.

[192] *UNSR Report, supra* note 186.

of rules (needed for successful DPI- or DNS-based Internet shutdowns).[193] Furthermore, governments may prefer throttling because, as a subtler shutdown tactic, it exhibits the same as would unintentional technological errors, overloaded infrastructures, or cyberattacks by non-state actors.[194] Thus, throttling may make it easier for governments to avoid accountability for the shutdown as it cannot as easily be pinpointed to a State action without evidence of a throttling order.[195]

III. HUMAN RIGHTS VIOLATIONS THAT ARE MOST LIKELY TO RESULT FROM AN INTERNET SHUTDOWN

The international human rights community recognizes that access to the Internet is a necessary precondition for the exercise and enjoyment of many human rights, both online and offline.[196] The United Nations Human Rights Council (HRC), an inter-governmental body that is the highest level of the United Nations' human rights machinery,[197] has consistently affirmed that "the same rights that people have offline must also be protected online."[198] The United Nations' (UN) advocacy regarding rights-based principles for Internet governance dates as far back as 2008, with the founding of the Internet Rights & Principles Dynamic Coalition (IRP Coalition), an open network of individuals and non-governmental organizations (NGO) based out of the UN Internet Governance Forum, that continues this important work today.[199] In Europe, the Committee of Ministers of the Council of Europe has stated that "[a]ccess to the internet is a precondition for the exercise of rights and freedoms online," as enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms.[200] Likewise, the Inter-American Commission on Human Rights (IACHR) has stated that the Internet "is a condition *sine qua non* for the effective exercise of human rights today, especially including the rights to freedom of expression and opinion, association and assembly."[201] The African Commission on Human and People's Rights (ACHPR) agreed, saying that "states shall

[193] *Internet Society Perspectives on Internet Content Blocking, supra* note 120.
[194] Wall Street Journal, *supra* note 110.
[195] *Id.*
[196] Clément Voule, *Ending Internet Shutdowns: A Path Forward, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association* (June 15, 2021), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/149/66/PDF/G2114966.pdf?OpenElement (hereinafter "Ending Internet Shutdowns: A Path Forward").
[197] *Instruments and Mechanisms,* UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER, https://www.ohchr.org/en/instruments-and-mechanisms [https://perma.cc/ZF9S-NUAT] (last visited March 3, 2023).
[198] *Ending Internet Shutdowns: A Path Forward, supra* note 196.
[199] *The Charter of Human Rights and Principles for the Internet*, UNITED NATIONS HUMAN RIGHTS COUNCIL, 3, 2014, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf [https://perma.cc/MU6K-93NE] (last visited Mar. 3, 2023); *see also Internet Rights & Principles Coalition*, https://internetrightsandprinciples.org/ [https://perma.cc/Z2AX-QXLL] (last visited Mar. 3, 2023).
[200] *Ending Internet Shutdowns: A Path Forward, supra* note 196.
[201] *Id.*

recognize that universal, equitable, affordable and meaningful access to the internet is necessary for the realization of freedom of expression, access to information and the exercise of other human rights."[202]

The international human rights community has specifically spoken out against state-sanctioned Internet shutdowns. In a June 2016 resolution, the HRC stated that measures aimed at preventing or deliberately disrupting access to information or the dissemination of information online are an international human rights law violations.[203] The resolution called on all states to refrain from, and end, such practices.[204] More recently, in the 2020 Roadmap for Digital Cooperation, the UN Secretary-General stressed that "blanket internet shutdowns and generic blocking and filtering of services are considered by UN human rights mechanisms to be in violation of international human rights law."[205] That same year, the Human Rights Council resolution on human rights in the context of peaceful protests adopted stronger language against shutdowns.[206] Additionally, the U.N. General Assembly and the Human Rights Council have both called upon States to refrain from implementing internet shutdowns.[207] Regional human rights law authorities have also emphasized Internet shutdowns' infringement on human rights. For example, the African Commission on Human and People's Rights specifically mentioned shutdowns in Chad, Sudan, Democratic Republic of the Congo, Gabon, and Zimbabwe that had occurred in the preceding year in a January 2019 press release.[208] Another example is the Economic Community of West African State (ECOWAS) Community Court of Justice, which in June 2020, upheld that the 2017 Internet shutdown by the Togolese government violated human rights.[209] As a final example, the Council of Europe called on States to recognize that disconnecting Internet access disproportionately restricts the right to freedom of expression.[210]

Potential human rights violations resulting from government-mandated Internet shutdowns can be assessed under the Universal Declaration of Human Rights (UDHR) and the International Covenant on

[202] *Id.*

[203] *Chad: Internet shutdowns impeding freedom of expression*, AMNESTY INTERNATIONAL (Apr. 2, 2021), https://www.amnesty.org/en/latest/press-release/2021/04/tchad-les-coupures-internet-une-entrave-la-liberte-dexpression/ [https://perma.cc/5T69-7XUH].

[204] *Id.*

[205] *Ending Internet Shutdowns: A Path Forward, supra* note 196.

[206] *Ending Internet Shutdowns: A Path Forward, supra* note 196; G.A. Res. 44/20, at 4 (July 23, 2020).

[207] *Ending Internet Shutdowns: A Path Forward, supra* note 196.

[208] *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*, AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS (Jan. 28, 2019), https://achpr.au.int/en/news/press-releases/2019-01-29/press-release-special-rapporteur-freedom-expression-and-access [https://perma.cc/J94B-NMQY].

[209] Natalia Krapiva, *ECOWAS Togo court decision: Internet Access is a Right that Requires Protection of the Law*, ACCESS NOW (July 14, 2020), https://www.accessnow.org/ecowas-togo-court-decision/ [https://perma.cc/CYB6-FCG3].

[210] *Ending Internet Shutdowns: A Path Forward, supra* note 196 (citing Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom).

Economic, Social, and Cultural Rights (ICESCR).[211] The majority of discussions of human rights violations resulting from Internet shutdowns revolve around three fundamental human rights: freedom of expression, freedom of assembly, and the right to life. These discussions also incorporate the variety of economic, social, and cultural rights which could be violated as a result of the Internet's ubiquity in modern life.

A. Freedom of Expression

One of the human rights most closely associated with the Internet is freedom of expression as detailed in Article 19 of both the UDHR and ICCPR. Freedom of expression is a fundamental human right and includes the "freedom to hold opinion without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[212]

Human rights experts and institutions have recognized and raised to the attention of the global community how the Internet and the right to freedom of expression are inexorably linked. David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression from August 2014 until July 2020, extensively discussed the interplay between the Internet and freedom of expression.[213] Kaye was not the first UN Special Rapporteur to link the Internet's uniquely transformative nature with the need to protect the right to freedom of expression: Frank La Rue delivered a Special Report to the Human Rights Council in 2011 on the topic.[214] The Inter-American Special Rapporteur for freedom of expression, Catalina Botero Marino, similarly advocated for the acknowledgment of the unavoidable link between the Internet and the right to freedom of expression in her report on this topic to the Inter-American Commission on Human Rights in 2014.[215] More recently, in 2019, Lawrence Murugu Mute, then African

[211] *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71, https://www.un.org/en/about-us/universal-declaration-of-human-rights [https://perma.cc/77RZ-XMW7]; Nations (General Assembly), (1966). *International Covenant on Economic, Social, and Cultural Rights.* Treaty Series, 999, 171, https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx [https://perma.cc/TGQ3-7KB4].

[212] *Universal Declaration of Human Rights, supra* note 211, at Article 19.

[213] *UN Expert Demands Urgent Boost for Online Rights Amid Rampant State Censorship*, UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER (Jun. 12, 2017), https://www.ohchr.org/en/press-releases/2017/06/un-expert-demands-urgent-boost-online-rights-amid-rampant-state-censorship [https://perma.cc/FC3M-UHNE]; *Special Rapporteur's June 2017 Report to the Human Rights Council*, FREEDEX.COM, https://freedex.org/the-special-rapporteurs-june-2017-report-to-the-human-rights-council/ [https://perma.cc/3PEC-8WNF].

[214] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (2011), https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [https://perma.cc/T2U5-VFEW].

[215] Catalina Botero Marino, *Freedom of Expression and the Internet, Special Rapporteur for Freedom of Expression,* INTER-AMERICAN COMMISSION ON HUMAN RIGHTS (Dec. 31, 2013), http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf [https://perma.cc/4Y38-M5US].

Commission on Human and Peoples' Rights' Special Rapporteur on freedom of expression and access to information in Africa, specifically discussed Internet shutdown tactics as a means of disrupting freedom of expression.[216] He stated that citizens should not be penalized by Internet shutdowns when demonstrating, calling for reforms, or during elections.[217] Amnesty International likewise considers Internet shutdowns to be a repression of freedom of expression.[218]

Furthermore, two Joint Declarations have highlighted how the Internet and freedom of expression are linked and have explicitly denounced Internet shutdowns.[219] The first of these Joint Declarations, from 2017, was created by The United Nations 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.[220] It stated that "cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public . . . can never be justified, including on public order or national security grounds."[221] The same applies to slow downs imposed on the Internet or parts of the Internet."[222] In 2019, the same group released a Twentieth Anniversary Joint Declaration on Challenges to Freedom of Expression in the Next Decade.[223] The Declaration demanded states refrain from Internet shutdowns or intentional telecommunications network disruptions in order to create an environment that enables the exercise of freedom of expression."[224]

B. Freedom of Assembly

The right to freedom of assembly, as detailed in Article 21 of the UDHR, is the other human right most commonly associated with the Internet due to the technology's use in organizing and facilitating

[216] *Chad: Internet shutdowns impeding freedom of expression, supra* note 203.

[217] *Id.*

[218] *Id.*

[219] *Joint Declaration on Challenges to Freedom of Expression in the Next Decade*, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (July 10, 2019), https://www.osce.org/representative-on-freedom-of-media/425282 [https://perma.cc/GQ54-L7FK]; *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda*, ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (Mar. 3 2017), https://www.osce.org/fom/302796 [https://perma.cc/Q9TN-KWVV].

[220] *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda, supra* note 219.

[221] *Joint Declaration on Freedom of Expression and the Internet,* ORGANIZATION OF AMERICAN STATES (June 1, 2011), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=848 [https://perma.cc/VEP7-BYHE].

[222] *Joint Declaration on Challenges to Freedom of Expression in the Next Decade*, *supra* note 219.

[223] *Joint Declaration on Challenges to Freedom of Expression in the Next Decade, supra* note 219.

[224] *Id.*

demonstrations. An expansive understanding of the right to peaceful assembly has been traditionally encouraged by the human rights community, and full exercise of this right should be considered normative while restrictions upon this right should be a rare exception.[225] This expansive understanding should include how digital spaces contribute to peaceful assembly, as indicated in General Comment No. 37 of the Human Rights Committee on Article 21, which reads: "Although the exercise of the right of peaceful assembly is normally understood to pertain to the physical gathering of persons, Article 21 protection also extends to remote participation in, and organization of, assemblies, for example, online."[226]

As with freedom of expression, human rights experts have asserted that the Internet and Article 21 are implacably linked.[227] In June 2020, the UN High Commissioner for Human Rights released a report on the impact of new technologies, including the Internet, on the promotion and protection of human rights in the context of assemblies, including peaceful protests.[228] In it, the Commissioner concluded "the use of [new] technologies to surveil or crack down on protesters can lead to human rights violations, including infringement of the right to peaceful assembly."[229] The year before, in 2019, the UN Special Rapporteur on the rights to freedom of peaceful assembly and association, Clement Voule, directly acknowledged the growing problem of Internet shutdown on the rights to freedom of peaceful assembly and of association in the digital era. Voule warned that "[n]etwork disruptions amid peaceful assemblies" had "become a dangerous global trend."[230] Two years later, in June 2021, Special Rapporteur Voule released a UNSR Report specific to the growing trend of Internet shutdowns, the dangers they pose to human rights, and how they interact with Article 21.[231] The 2021 report was a follow-up to the 2019 report.[232]

[225] *Ending Internet Shutdowns: A Path Forward, supra* note 196.

[226] *Id.*

[227] Ilia Siatita, *Freedom of Assembly Under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications*, INTERNATIONAL REVIEW OF THE RED CROSS, No. 913 (March 2021), https://international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-913 [https://perma.cc/KVR9-SG6W]; *see also UN Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including Peaceful Protests*, UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, UN Doc. A/HRC/44/24 (24 June 2020); *see also The Rights to Freedom of Peaceful Assembly and of Association*, HRC Res. 15/21 (6 Oct. 2010); *see also* Maina Kiai & Jeff Vize, *Three Years after Tunisia: Thoughts and Perspectives on the Rights to Freedom of Assembly and Association from United Nations Special Rapporteur Maina Kiai*, JOURNAL OF GLOBAL ETHICS, Vol. , No. 1 (2014).

[228] *UN Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including Peaceful Protests*, *supra* note 227.

[229] Siatita, *supra* note 227.

[230] *UNSR Report, supra* note 186.

[231] *Ending Internet Shutdowns: A Path Forward, supra* note 196.

[232] *Ending Internet Shutdowns: A Path Forward, supra* note 196.; see also *Rights to Freedom of Peaceful Assembly and of Association, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association,* A/HRC/41/41 (May 17, 2019), https://www.ohchr.org/en/documents/thematic-reports/ahrc4141-rights-freedom-peaceful-assembly-and-association-report-special [https://perma.cc/W4QN-QAP9].

C. Right to Life

Article 2 of the UDHR protects the right to life.[233] There are two ways in which Internet shutdowns can contribute to a violation of Article 2. First, an Internet shutdown might result in lack of information necessary for life to be sustained.[234] Second, the unfortunate reality is that government-led Internet shutdowns often precede or coincide with atrocities.[235] An Internet shutdown can be a tactic used concurrently with other actions by the government that violate the right to life as a means of slowing the flow of information about the atrocities or by obstructing documentation of the atrocities and other digital forms of government accountability (such as livestreaming).[236]

The Internet has become the place we go to for immediate, fast information. In times of crisis, whether personal, local, or otherwise, our first instinct is to turn to the Internet for help or information. When Internet access is shutdown, access to life-saving information might be blocked, resulting in a loss of life.[237] One tragic example of this can be seen in Pakistan, where a woman experiencing pregnancy complications during an Internet shutdown was not able to contact her doctor and lost her child as a result—an occurrence for which there are likely many more examples, but little documentation.[238] More recently, the human rights community has denounced government-mandated Internet shutdowns that occurred during the global COVID-19 pandemic, a time when information was vital not only to individual health but also to public safety.[239] Internet shutdowns during the pandemic impeded people's ability to access essential services and intensified the closing of civic space during this health crisis.[240]

Even more horrifying are the large-scale shows of force and violence that are regularly enacted by states against their populations during times when they have ordered an Internet shutdown.[241] This pervasive pattern of shutdowns and atrocities cannot be understated; non-exhaustively, Internet shutdowns have coincided with government-led mass killings of civilians in Myanmar in 2007, 2017, and again in 2021; Iran in 2009 and 2019; Egypt in 2011; Sudan in 2013 and 2019; the Central African Republic in 2014; Ethiopian in 2016 and 2020; and Iraq in 2019.[242]

[233] *Universal Declaration of Human Rights*, *supra* note 211.

[234] Kaye, *supra* note 9, at 12.196

[235] Wall Street Journal, *supra* note 110.

[236] Kaye, *supra* note 9, at 12.

[237] *Id.*

[238] *Id.* at 12.

[239] *Ending Internet Shutdowns: A Path Forward, supra* note 196.

[240] *Id.*

[241] Kaye, *supra* note 9, at 12.

[242] Kaye, *supra* note 9, at 12-13; *Ending Internet Shutdowns: A Path Forward, supra* note 196.

D. Economic, Social, and Cultural Rights

Economic, social, and cultural human rights (ECSHRs) ensure that all people can access basic goods, services, and opportunities necessary to survive and thrive.[243] ECSHRs are primarily defined by the ICESCR.[244] The International Convention on Civil and Political Rights (ICCPR) further defines several economic, social, and cultural human rights.[245] Other socio-economic human rights have been likewise defined or emphasized in topic-specific Conventions and region-specific Charters.[246] Economic rights as a classification are somewhat controversial, but in particular the right to work and the right to unionize are commonly considered invokable economic rights (UDHR Article 23).[247] Social rights are human rights which meet the basic needs essential for human welfare, including the right to health (ICESCR Article 12) and to education (Article 13).[248] Cultural rights allow one to take part in cultural life, such as enjoying the benefit of scientific process and the right to intellectual property (UDHR Article 27).[249] Some additional examples of ECSHRs have been interpreted to include having the right to vote (UDHR Article 21), the right to mental, physical, and sexual health information (ICESCR Article 12), and the right of minorities to engage in their respective cultures and religions (UDHR Article 27), to name a few.[250] As with other human rights, modernity intertwines the Internet with ESCHRs and Internet shutdowns may violate ESCHRs as a result.

[243] *Measuring Economic & Social Human Rights,* HUMAN RIGHTS MEASUREMENT INITIATIVE, https://humanrightsmeasurement.org/methodology/measuring-economic-social-rights/#:~:text=Economic%20and%20social%20human%20rights,necessary%20to%20survive%20and%20thrive [https://perma.cc/6K4V-ZE3L] (last visited Apr. 10, 2023).

[244] *Int'l Covenant on Economic, Social, and Cultural Rights, supra* note 211.

[245] *Int'l Covenant on Civil and Political Rights*, Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1973), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights [https://https://perma.cc/47AW-6D5G].

[246] For example, The Convention on the Elimination of All Forms of Racial Discrimination prohibits discrimination on the basis of racial and ethnic origin. Regional Charters tend to mirror rights granted in the known authoritative documents (such as the right to work, the right to health, etc). *Int'l Convention on the Elimination of All Forms of Racial Discrimination*, Dec. 21, 1965, 660 U.N.T.S. 195 (entered into force Jan. 4, 1969), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial [https://perma.cc/KK5P-D69J].

[247] Rotem Litinski, *Economic Rights: Are They Justiciable, and Should They Be?*, A.B.A. HUMAN RIGHTS MAGAZINE (Nov. 30, 2019), at 23, https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/economic-justice/economic-rights--are-they-justiciable--and-should-they-be-/ [https://perma.cc/T4YV-YGPN].

[248] Virginia Mantouvalou, *The Case for Social Rights*, GEORGETOWN PUB. L. RESEARCH (May 17, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588220.

[249] Note that some rights defined in the ICESCR are also defined in the UDHR. *Universal Declaration of Human Rights, supra* note 211; *Int'l Covenant on Economic, Social and Cultural Rights, supra* note 211.

[250] *Universal Declaration of Human Rights, supra* note 211; *Int'l Covenant on Economic, Social and Cultural Rights, supra* note 211.

1. The Economic Impact of Internet Shutdowns

The economic argument against Internet shutdowns is easy to make; substantial economic research has shown the negative impact of Internet shutdowns, and how intentional network disruptions significantly damage the financial ecosystem and local economy of their impact zones.[251] It is estimated that every day of complete Internet blackout in a high-connectivity country would result in an average loss of $23.6 million per ten million in the population.[252] Medium-connectivity countries, comparatively, would lose $6.6 million.[253] Overall, in 2022, Internet shutdowns cost the global economy $24 billion.[254] Like other aspects of shutdowns, this data has remained consistent: The Brookings Institution estimated that in 2015 alone, Internet shutdowns had cost the world economy $2.4 billion.[255] Of that, half the damage to GDP came from one offender: India, the most major implementor of Internet shutdowns annually for the last five consecutive years.[256] In 2016, intentional network disruptions in Sub-Saharan Africa cost the regional economy more than $218 million.[257] As outlined in a five-year economic report by the Indian Council for Research on International Economic Relations, the economic impacts of Internet shutdowns are felt across varied populations within the restricted region: individual workers, students, businesses, and even government officials.[258]

These numbers are powerful and tangible depictions of harms caused by Internet shutdowns, but they aren't the whole picture of a shutdown's impact. The risk in looking at shutdowns purely through an economic lens is that it could give the illusion that certain types of shutdowns are more acceptable than others because of their lesser economic impacts.[259] For example, a digital curfew keeps the Internet "open for business" during the day and allows people to continue to work while restricting Internet access at night when users and activists are more likely to gather to

[251] Kaye, *supra* note 9, at 13-14; Jeremy Hsu, *How India, The World's Largest Democracy, Shuts Down the Internet*, IEEE SPECTRUM (Jan. 27, 2020), https://spectrum.ieee.org/how-the-worlds-largest-democracy-shuts-down-the-internet [https:// https://perma.cc/R6HJ-D522]; Rydzak, *supra* note 8, at 15-16.

[252] Rydzak, *supra* note 8, at 15-16.

[253] *Id.*

[254] Sebastian Klovig Skelton, *Internet Shutdowns Cost Global Economy $24bn in 2022*, COMPUTERWEEKLY.COM (Jan. 11, 2023), https://www.computerweekly.com/news/252529078/Internet-shutdowns-cost-global-economy-24bn-in-2022 [https:// https://perma.cc/W4Q7-H45J].

[255] Rydzak, *supra* note 8, at 16.

[256] Rydzak, *supra* note 8, at 15-16; Skelton, *supra* note 253.

[257] Rydzak, *supra* note 8, at 16.

[258] Rajat Kathuria et al., *The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India*, INDIAN COUNCIL FOR RESEARCH ON INTERNATIONAL ECONOMIC RELATIONS (April 2018), https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf, [https://perma.cc/UBF4-3QEN].

[259] Kaye, *supra* note 9, at 14.

communicate.[260] As such, it has a lesser economic impact and is less likely to violate one's right to work (ICESCR Article 6). But it is important to remember that no intentional Internet shutdown is acceptable. Digital curfews and other Internet restrictions that allow some levels of commerce to continue still infringe fundamental human rights, such as freedoms of opinion and expression.[261] Although making the economic argument against shutdowns may seem straightforward and appealing, fiscal damages and the violation of economic rights must be considered alongside the violation of other human rights.

CONCLUSION

It is understandable why advocating for Internet access as a human right has appealed to anti-shutdown activists. As seen in this installment, Internet shutdowns may be implemented in a wide variety of ways and there are several human rights which may or may not be violated by a shutdown. Technologically, shutdowns can be difficult to understand, and when enacted without transparency, can be hard to identify as intentional acts by authorities. It might seem simpler, then, to advocate for a "new right" rather than dissecting on a case-by-case basis how a particular shutdown may have caused harm. Furthermore, it might seem as though better protections could be put in place if States were explicitly obligated to comply with a human right to the Internet, or if shutdowns were more directly identified as a human rights violation in and of themselves. But this is not the case. It is because of the nuances of Internet shutdowns that a fact-based, case-by-case approach is needed to establish accountability for its resulting harms.

If lawyers and activists strategically select individual human rights violations claims to bring before impact-minded supervisory bodies, then the focus continues to be on the harms rather than the mechanisms for those harms. This approach is beneficial for two reasons. Firstly, it allows lawyers and activists to rely on established case precedence. This, then, allows for more predictable, reliable outcomes in terms of remedies for those harmed and sanctions against the offending State. It also establishes unambiguous obligations for States' actions, and more quickly, than the resulting nebulous obligations that may come with States' agreement to recognize a new human right—if they choose to recognize it at all. Secondly, this approach establishes a trend in which other technologies, such as surveillance drones or problematic machine learning algorithms, can likewise have claims of violations brought under classical human rights. Ideally, this results in a swifter redress for harms as it does not rely on the arduous and unpredictable process of attempting to get a new right recognized by the international human rights community. It also eliminates the need to establish a new human right with each wave of

[260] *Id.*
[261] *Id.*

evolved technologies utilized inappropriately by governments against their citizens.

As will be discussed in the next installment, Resolutions that have condemned shutdowns or stated that Internet access is a human right have had no discernable effect on decreasing the frequency or intensity of shutdowns. So, too, is the case with localized Human Rights-Based Approaches to policies condemning shutdowns. State-sanctioned Internet shutdowns continue to be wielded by governments as a weapon of control and oppression against their own populations regardless of these "wins." However, attempts to hold States accountable for Internet shutdowns in the Courts are growing in popularity. With the right legal strategy, a claim could successfully be brought against an offending State for its patterns of Internet shutdowns and the resulting human rights violations. The upcoming installment will discuss the few existing cases brought against States for their shutdowns and detail their successes and failures. The installment will show why bringing Internet shutdown-based human rights violation claims to supervisory bodies in impact-focused jurisdictions is a necessary step in beginning to curb this harmful practice used by technology-wielding governments around the world.