ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Case for a Mostly Open Internet

MICHAEL MCLAUGHLIN AND DANIEL CASTRO I DECEMBER 2019

Policymakers should seek to maximize the benefits of Internet openness while maintaining carefully designed guardrails that reduce the Internet's most clearly harmful uses.

KEY TAKEAWAYS

- The general openness of the Internet supports economic growth by increasing international trade, productivity, employment, and innovation.
- However, increasingly some nations are limiting Internet openness in ways which will harm economic growth.
- At the same time the Internet has never been fully open. Governments have long blocked illicit and dangerous material such as terrorist propaganda, pirated content, and malware.
- Too little openness limits the economic and social value of the Internet. Too much openness allows harmful activity. However, a "mostly" open Internet can maximize the value of the Internet.
- Policymakers should seek to maximize Internet activities that are universally regarded as good, reduce activities universally regarded as bad, and create a high level of technical openness.

INTRODUCTION

The general openness of the Internet has generated tremendous economic and social value, giving users the freedom to connect, speak, innovate, and share content without restrictions. Unfortunately, many countries have in recent years enacted policies that undermine this openness.[1] In 2018 alone, at least 25 nations throttled down users' bandwidth, shut off their mobile or broadband Internet services altogether, or blocked access to mainstream Internet sites or applications.[2] More recently, Russia enacted a law requiring domestic Internet Service Providers (ISPs) to route traffic through government-managed servers, which could allow the government to cut off all foreign network traffic while maintaining access to popular domestic online services.[3] Meanwhile, Singapore has passed a law requiring online services to take down content domestically the government deems to be false, and Vietnam has passed a law requiring online services to remove content removed the government deems offensive.[4]

Governments have rationalized these policies as being necessary solutions to such difficult challenges as protecting national security, securing elections, and quelling violence and social unrest.[5] But on net, such measures are costly, both economically and socially—and often cause harms worse than the problems governments want to address.[6] For example, policies that impede Internet access or otherwise limit firms' ability to leverage the Internet—such as requiring data to be stored locally—reduce competition and digital trade, increase costs for consumers and businesses, and limit nations' ability to use the Internet to innovate.[7] In the case of shutting down access to the Internet entirely, or blocking access to major applications, there are clear economic costs. For example, the Indian Council for Research on International Economic Relations (ICRIER) has estimated that more than 16,000 hours of government-mandated shutdowns of mobile or fixed-line Internet access cost the nation's economy $3 billion between 2012 and 2017.[8]

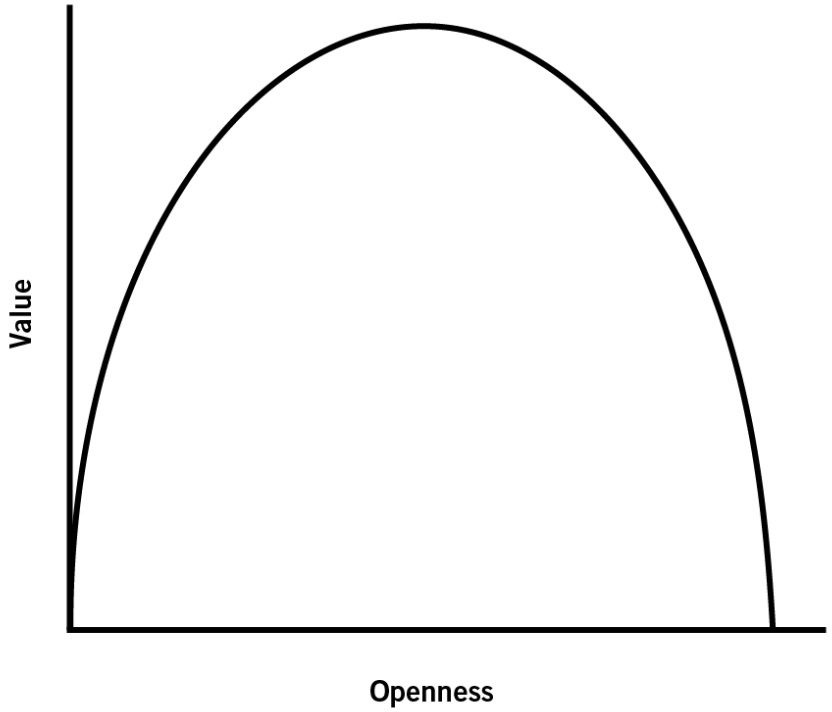
The unabated stream of Internet shutdowns, data localization policies, and decisions to block websites and online services show that some policymakers do not clearly understand or properly value the benefits of a mostly open Internet.

Yet the unabated stream of Internet shutdowns, data localization policies, and decisions to block websites and online services show that some policymakers do not clearly understand or properly value the benefits of a mostly open Internet. To be clear, the Internet has never been fully open—nor should it be—as governments have long blocked illicit and dangerous material such as terrorist propaganda, pirated content, and malware. But there are also many recent examples of state intervention in innocuous Internet activity undermining economic growth and social progress. To give policymakers an analytical perspective on the issue, this report presents a conceptual framework for assessing the economic and social value of the Internet in relation to its openness. The report also provides concrete examples of the costs associated with a more closed Internet.

There are multiple ways to gauge the value of Internet openness, including by breaking down the overall value of the Internet into the economic value and social value it generates—which reveals not just that the mostly open Internet is tremendously valuable, but also that there is a limit to how much additional value the Internet can produce for society by continuing to become more

open. Indeed, policymakers should think of the value of the open Internet as an inverted U curve. With too little openness, the economic and social well-being the Internet can provide is severely limited. With the right amount of openness, the Internet maximizes its value. And with too much openness, the Internet creates significant drawbacks, thereby reducing its economic and social value. Examples include allowing the sale of widely banned drugs and doing nothing to prevent child exploitation online. Clearly, nations should not blindly pursue maximum Internet openness; they should instead embrace openness for what most democracies would consider to be legal and ethical applications.

Figure 1: Internet openness versus Internet value



It is worth noting there are important limitations to thinking about the value of the open Internet as an inverted U. First, there is no definitive way to measure how much more or less open a policy or condition makes the Internet. Consequently, it is difficult to precisely place a policy or condition on the inverted U. Second, policies that affect Internet openness are rarely substitutes for one another. Some conditions, such as allowing data to flow freely between nations, have limited value unless everyone uses consistent technical standards. Third, a monolithic inverted U would not reflect how a policy or condition actually affects Internet openness or is valued differently by separate groups. For example, privacy regulations can increase Internet openness for consumers if they encourage users to engage in more activities online, but can decrease Internet openness for businesses if the regulations limit how businesses may collect and use data to innovate.[9] Nonetheless, many nations—especially developing economies—have positioned themselves on the upward slope of the U with their policies, wherein more openness would lead to greater welfare.

This report argues policymakers should seek to maximize the benefits of Internet openness while maintaining carefully designed guardrails that reduce damaging uses of the Internet. Policymakers should also encourage ISPs to continue to evolve and improve their networks in order to support new services. The key debate should therefore focus on which policies maximize the benefits of Internet openness, and which policies nations should pursue even if they reduce Internet openness. The challenge for lawmakers is to position their nations on the top of the inverted U, where Internet openness produces maximum value. In practice, this entails promoting an open Internet in most situations, while also prohibiting activities society deems unacceptable. However, governments' right to guard against these universal harms by limiting access to certain material cannot be a cover or justification for censorship. Moreover, it is in the interest of democratic nations, both morally and economically, to push for the adoption of policies such as freedom of expression that increase Internet openness internationally. Indeed, this report does not support efforts to increase governments' ability to criminalize ordinary online activities. For example, it opposes the recent efforts of some nations to pass a United Nations resolution attempting to normalize increased state control of the Internet.[10] In addition, Chinese president Xi Jinping has argued nations "should respect the right of individual countries to independently choose their own path of cyber-development." While this report concedes nations should have the right to set their own domestic policy, it does not endorse inappropriately limiting basic Internet freedoms—such as free speech—most democracies consider to be near-universal goods.[11]

Policymakers should seek to maximize the benefits of Internet openness while maintaining carefully designed guardrails that reduce damaging uses of the Internet.

This report first defines the open Internet, and then outlines threats to the open Internet, before discussing the economic value of a mostly open Internet. Next, it discusses the cost of reducing Internet openness. Finally, the report provides an analytical framework policymakers can use to evaluate policies that affect Internet openness.

WHAT IS THE OPEN INTERNET?

To highlight the relevancy of the open Internet, this section outlines some of the threats the Internet faces. In general, the "open Internet" refers to the concept of allowing all the various users and stakeholders in the Internet ecosystem the opportunity to connect, speak, innovate, share, and offer new services without undue restriction. This framework is broader than the narrow concept of network neutrality, which is focused on the actions of ISPs, and how blocking, throttling, and unfair prioritization of Internet traffic could negatively affect the openness of the Internet.[12] Net neutrality violations have been relatively rare; however, other threats to Internet openness—usually undertaken by a government actor acting in concert with network operators—are on the rise.

Using this report's definition, the Internet is more or less "open" depending on the interplay between technical, business, and political factors.[13] For example, open technical protocols such as transmission control protocol/Internet protocol (TCP/IP) increase Internet openness by facilitating the communication of different computers.[14] In addition, a uniform convention for domain names increases openness by ensuring users connect to their intended websites. Internet

openness also increases as more websites follow the World Wide Web Consortium's accessibility standards by facilitating the use of the Internet by people with disabilities.[15] However, increasing the openness of the Internet can also include allowing harmful online activity, such as the sale of widely banned drugs, distribution of malware, and unauthorized copying or streaming of copyright-protected content. Yet every nation restricts at least some malicious uses of the Internet, just as they impose restrictions on activity in the physical world. There is no justification for "Internet exceptionalism"—the belief the Internet is so unique, traditional rules should no longer apply. The Internet has never been fully open—nor should it be.[16]

The Internet can also become more closed in several ways. Hackers can engage in denial-of-service attacks that make particular websites inaccessible. ISPs can block or throttle certain Internet traffic, such as Voice over Internet Protocol (VoIP) or other messaging services. Governments can order firms that control the Internet's infrastructure, such as the physical cables that transmit information, to fully turn off Internet access. In nations where Internet traffic travels through only a few facilities, the process of cutting off access to the global Internet can be as simple as turning off the power at those hubs.[17] In addition, governments can require ISPs to block access to specific mainstream websites or Internet applications. Policymakers can also reduce openness by passing legislation that limits or deters freedom of expression online. For example, Egypt's parliament passed a bill in 2018 that classifies social media users with more than 5,000 followers as "media outlets," which allows the government to prosecute them for publishing what it deems to be false.[18]

If all efforts to reduce Internet openness are labeled as bad—even reasonable ones designed to limit harmful and unethical practices—then nations engaging in unreasonable practices can dismiss those calling for necessary and appropriate openness as having an ideological bias.

The conventional wisdom about the open Internet that "more is better" has had some positive effects by setting an expectation at the technical, business, and policy level that Internet openness is critical and something to be pursued. Indeed, this core openness is a major reason the world has seen the flourishing of the Internet and all its myriad and beneficial applications over the last two decades. But at the same time, framing the issue as more openness always being better has led some individuals and groups to oppose policies that would hurt Internet openness but have positive outcomes. This absolutist framing actually makes it harder—not easier—to challenge authoritarian regimes that engage in harmful efforts to create a more closed Internet. If all efforts to reduce Internet openness are labeled as bad—even reasonable ones designed to limit harmful and unethical practices, or improve the functionality of the network for new services—then nations engaging in unreasonable practices can dismiss those calling for necessary and appropriate openness as having an ideological bias.[19]

A closer look shows context matters. For example, website blocking reduces Internet openness. But whether this blocking is positive or negative depends on the types of websites being blocked. Governments blocking mainstream news sites is a clear restriction on a free press, and has a negative impact on society's ability to be informed, debate ideas, and hold leaders accountable. On the other hand, governments blocking foreign sites that, for example, sell tainted infant formula, has both a clear benefit to domestic consumers and a positive impact on the value of the Internet. As a result, policymakers should reject the narrative that implies the choice

between an open and closed Internet is a binary one. Instead, their goal should be to foster a mostly open Internet in which users are able to receive its social and economic benefits while also being shielded from its clearly negative uses.

HOW IS THE "OPEN INTERNET" THREATENED?

Threats to the open Internet can be broken down into three general categories: technical, commercial, and governmental. Technical obstacles can limit people's ability to use the Internet. Commercial threats arise as a result of competitive dynamics that drive private actors to undermine openness in the Internet ecosystem. Governmental threats, whereby sovereign actors take steps to undermine Internet openness, are often the most pernicious, especially when undertaken in concert with closely regulated or nationalized Internet operators.

Technical Threats to Internet Openness

Technical threats include the slow transition from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). Each device connecting to the Internet needs its own IP address, but IPv4 can only provide roughly 4 billion unique addresses.[20] Consequently, the supply of available IP addresses is limited. Meanwhile, although IPv6 can accommodate 3.4×10^{38} addresses, organizations have been slow to upgrade the necessary Internet infrastructure to IPv6 due to the cost.[21] While network-address translators have helped combat this issue by allowing multiple devices to share the same IP address, companies will eventually have to transition to using IPv6. There are also technical threats that are the result of vulnerabilities, such as in the domain name system—which translates domain names into IP addresses. Bad actors can use cache poisoning to replace the legitimate IP address of a website in a server's cache with the address of a malicious website.[22] This process can redirect users to malicious websites.[23]

Commercial Threats to Internet Openness

Commercial threats, whereby companies undermine the openness of the Internet in order to gain competitive advantage, are thankfully rare in most developed nations. There is a long history of regulators and telecommunications providers coordinating to block VoIP, especially in countries with extensive tariffing regimes, and where communications providers do not have flexibility to change the pricing of their services.

Telecommunications has extremely high up-front and ongoing operating costs for building or upgrading networks, but very low marginal costs for serving additional voice minutes, text messages, and data. Operators must price their services well above marginal costs in order to recoup their investment in building and operating the network. This leads to pricing that reflects services customers value—not necessarily the load on the network.[24]

VoIP and other messaging applications disrupt this pricing practice, allowing Internet-based companies to offer low-cost or free services over a general-purpose data connection. These other over-the-top (OTT) messaging and voice services offer great benefits to end users, and should therefore be welcomed; however, low-cost or free communications tools can make for a painful transition for some operators. Network operators have seen a significant decline in revenue from messaging and voice services, which has led regulators and telecommunications firms in some countries to block some VoIP and OTT applications.

In the United States, VoIP blocking is responsible for the only real net neutrality violation to date, when over 14 years ago, Madison River Communications—a small, local telephone company in North Carolina—attempted to block VoIP applications, such as Skype, that competed with its phone business from operating over its network.[25] Almost immediately after the resulting justified outrage, Madison River stopped blocking VoIP applications.[26]

In other countries, especially where either the communications operators are significantly controlled by the government, or price regulations do not allow operators to easily change their pricing practices, blocking is more common. Many countries have a history of either requiring a license to offer VoIP services, or blocking them outright.[27] While the blocking of VoIP has declined since its introduction, it continues today. For example, ISPs in the United Arab Emirates have blocked Skype several times, including as recently as this year; in 2016, Moroccan ISPs blocked access to VoIP applications due to a fear of lost revenue; and ISPs have lobbied governments to regulate OTTs in several African nations, including Kenya, Nigeria, and South Africa.[28]

ISPs should not be allowed to block or unfairly undermine Internet services that compete with their traditional offerings. In turn, they need both the flexibility to change their pricing practices and the ability to innovate around business models.

The debate over how to address OTT regulation more generally was a focus of a recent recommendation developed at the International Telecommunications Union (ITU), a body of the United Nations.[29] It recognized the interdependence of OTT and traditional telecommunications services, rightly noting that OTT providers increase the value of the connectivity telecommunications operators provide. Competition drives better service, and should not be held back for the sake of a legacy regulatory pricing model. ISPs should not be allowed to block or unfairly undermine Internet services that compete with their traditional offerings. But in turn, they need both the flexibility to change their pricing practices (likely increasing the price of data or basic connectivity) and the ability to innovate around new business models.

Government Threats to Internet Openness

The worst offenders blocking OTT services for competitive reasons often act in concert with the government. For example, the governments of Qatar and Saudi Arabia have blocked access to VoIP applications. These blocks were likely a form of protectionism, as the government is a majority owner in a leading telecommunications provider in each nation.[30] Such actions are a threat to the open Internet—and these latter examples highlight the most serious threats to the open Internet today come not from business, but from governments.

Internet Shutdowns and Application Blocks

Governments have reduced Internet openness by intentionally throttling Internet service, shutting down Internet access, and blocking online services such as WhatsApp. They have ordered both mobile and broadband ISPs to turn off Internet access, as well as ISPs to block access to specific websites and applications. In 2018, at least 25 nations hindered or shutdown access to the Internet or to a popular application in one of the aforementioned ways, often by ordering ISPs to cease operations or block access to specific services. The number of these disruptions is on the rise, increasing from 75 in 2016 to at least 190 in 2018.[31]

Shutdowns and application blocks range widely in duration. India, which has led the world in Internet shutdowns and application blocks since 2012 with at least 357, typically shuts down mobile Internet access in a district for less than 72 hours.[32] In contrast, Chad blocked access to social media websites for more than a year.[33] The disruptions also vary in their scope. In Africa, for instance, the disruptions are typically national. In the Asia Pacific region, on the other hand, the disruptions are usually local.[34] Governments have cut off access to the Internet for a variety of reasons, such as to stem protests, stop the spread of fake news, and safeguard public safety and national security.[35] However, some of these justifications do not hold up to scrutiny. For example, the Chadian government argued it had to block access to social media applications in order to maintain security.[36] In reality, the government likely ordered the block in order to undercut the mobilization of the government's critics.[37]

Kill Switches

Governments can also threaten Internet openness at the architectural level. For example, Russia has enacted a law requiring ISPs to install equipment specifically from the government that allows the latter to monitor and cut off Internet traffic.[38] The law also mandates providers have the means to disconnect Russia's Internet access to the rest of the world and route traffic only internally in an emergency.[39] If Russia were to sever itself from the global Internet, both Russian and global Internet users could be negatively affected. Cloud services outside the nation could stop working, and users outside of Russia could lose access to content hosted on servers in Russia.[40]

The United Kingdom has two laws—the Civil Contingencies Act and the 2003 Communications Act—that provide the U.K. government with the power to compel ISPs to cease their operations or close the Internet exchange points that allow them to connect to one another in order to share traffic.[41] The U.K. government may invoke these powers only in times of emergency.[42]

Data Localization

Another way governments are reducing Internet openness is through data localization policies. As of April 2017, 34 countries had data localization policies.[43] These policies often limit the flow of business, personal, and other types of data by requiring organizations to store data domestically. This requirement increases data storage costs and limits the ability of Internet users to access online products and services.[44]

Censorship

Website blocking is also on the rise in many countries. As ITIF has written, some of this is for legitimate reasons, such as blocking access to content that infringes on copyrights.[45] But much of it is for political reasons. For example, Egypt increased the number of websites it blocked from 2 in 2015 to more than 500 in 2018. This list includes independent media outlets' websites.[46] And since December 2018, Chinese authorities have shut down or removed at least 140,000 social media accounts and roughly 500,000 articles.[47] This censorship is in addition to China's Great Firewall, which has blocked certain IP addresses and domain names, including independent news organizations, since the late 1990s.[48] Moreover, between June 2017 and May 2018, at least 17 countries introduced policies that increased censorship or the penalty for violating existing censorship laws.[49] In March 2019, Russian president Vladimir Putin signed into law legislation that makes it a crime to publish "fake news."[50] Countries are also banning virtual private networks (VPNs), which use encryption to provide users a private connection over

the Internet in order to prevent local ISPs from monitoring their online activity. Eleven countries currently ban or restrict VPN usage. In China, for example, only government-approved VPN service providers may be used, with failure to comply resulting in fines of more than $2,000 dollars.[51] Because VPNs are frequently used to access blocked content, any bans and restrictions on them only reduce the openness of the Internet.

However, not all government policies that decrease openness also decrease the value of the Internet. A wide range of activities that occur online, such as the distribution of child pornography, malware, and copyright-infringing content, severely reduce the social value of the Internet. Nations around the world are using website blocking to limit the spread of such content. For example, the 190 members of the International Criminal Police Organization voted unanimously to promote the use of website blocking in order to fight child pornography; Australia blocks websites that spread malware; and more than 40 other nations block websites containing copyright-infringing content.[52]

There is a stark difference between a government that uses transparent means within an independent legal system to block access to content and one that is engaging in censorship to control its population.

Some argue that even the legitimate blocking of content helps totalitarian governments justify their own content blocks. However, there is a stark difference between a government that uses transparent means within an independent legal system to block access to content and one that is engaging in censorship in order to control its population.[53] Just as supporting bans on cross-border human trafficking does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of free speech.[54] Indeed, policymakers can both foster valuable online activities and minimize the Internet's use as a venue for illegal activity.

VALUE OF THE (MOSTLY) OPEN INTERNET

Persuading lawmakers to pursue a mostly open Internet requires demonstrating the value of Internet openness. Unfortunately, there is no definitive way to measure the value of the Internet to the economy and society, which makes it particularly challenging to quantify the impact of policies that make the Internet more open or closed. However, many of the primary benefits of the Internet require a minimum level of openness. For example, one benefit of the Internet is increased trade in services. This benefit requires the different computers that use the global Internet be able to communicate. The widespread use of open technical protocols makes establishing these communications easier, thereby increasing openness and the potential value of the Internet. Nonetheless, it is easier to measure the costs of closed policies, such as those that limit data flows.

This report first discusses the value of a mostly open Internet in general, and then analyzes the policies that reduce Internet openness and value. It focuses on the benefits derived from the Internet in the United States and certain European nations in order to establish the value of a mostly free Internet.[55] When possible, examples from other nations are provided in order to both show the value of the Internet is widespread and link Internet openness to its value. In the

following sections, this report examines the contributions of the Internet to gross domestic product (GDP), trade in services, productivity, employment, and innovation.

Gross Domestic Product

Numerous studies of nations in various stages of development have found the Internet contributes substantially to their economies. For example, the U.S. Bureau of Economic Affairs (BEA) analyzes the contributions of the U.S. digital economy. Its definition of the digital economy includes the infrastructure needed for a computer network to exist and operate, digital transactions that take place within the network, and the digital content users create and access.[56] While BEA's definition does not perfectly overlap with the Internet economy, it does capture significant portions of the value associated with the Internet. In 2017, the U.S. digital economy accounted for 6.9 percent, or nearly $1.4 trillion, of the nation's GDP.[57] In comparison, the wholesale trade, retail trade, and construction industries each contributed less to U.S. GDP.[58] The U.S. digital economy also has an outsized influence on the growth of the economy as a whole. In 2017, for example, the U.S. digital economy accounted for 25 percent of the 2.2 percent growth in real GDP.[59] Notably, BEA, which calculated the size of the digital economy by analyzing categories in the North American Industrial Classification System, only considered a category as part of the digital economy if the products and services that make it up are primarily digital. Therefore, the U.S. digital economy may be an even larger contributor to GDP than the figures above portray. For example, due to a lack of data, BEA cannot identify what portion of advertising revenue stems from free digital media such as YouTube or Facebook, and does not include the revenue from free digital media in its estimates.[60]

Studies also regularly find increased Internet access or usage correlates with increases in GDP.

Studies also regularly find increased Internet access or usage correlates with increases in GDP. For example, a 2012 study by the World Bank found a 10 percent increase in fixed broadband generates a 1.35 percent increase in per capita GDP for developing countries.[61] In addition, another study found a 10 percent increase in the number of Internet subscribers in India has led to a 2.4 percent increase in state per capita GDP growth.[62]

Trade in Services

One of the primary benefits of an open, connected Internet is an increase in international trade. By connecting buyers and sellers, the Internet creates global value chains and reduces transaction costs.[63] Indeed, in 2018, the United States exported over $71 billion in information and communication technology services.[64] Of those exports, $38 billion were for the use of intellectual property in computer software. The United States exported another $380 billion in service exports that were potentially information and communications technology (ICT) enabled.[65] These services include, but are not limited to, financial and insurance services.[66] Furthermore, the Internet has benefitted trade in developing nations. For example, a 2004 study found that increases in Internet penetration in developing countries correlated with increases in exports to developed countries.[67] Similarly, a 2015 study of the 57 nations comprising the Organization of Islamic Cooperation found a positive relationship between a nation's Internet usage and its international trade in services.[68]

The Internet has also helped small businesses become exporters. For example, a 2013 study found that 95 percent of eBay commercial sellers exported products. On average, the sellers exported to between 24 and 39 international markets. Consequently, many eBay sellers reached more markets than did traditional organizations—for instance, firms in South Africa only exported to five international markets.[69] Lastly, more than half the firms that used the now-defunct Safe Harbor framework, which allowed businesses to transfer personal data from the European Union to the United States, had fewer than 100 employees.[70] These small businesses' participation demonstrated that the free flow of data, which increases Internet openness, was important to them. Indeed, a 2013 study estimated United States services exports to the European Union would fall by as much as 0.5 percent if the Safe Harbor Framework no longer existed. EU firms' exports would have dropped by 0.6 to 1.0 percent.[71] The EU-U.S. Privacy Shield—a framework that facilitates the flow of personal data between the European Union and the United States—has since replaced the Safe Harbor Framework.[72]

Productivity

Several studies have found a link between increased productivity and the Internet across sectors—although the level of productivity increases can be contingent on a range of factors, such as a firm's business model, employee skills, and reaching a critical mass of employees with Internet access. For example, a 2005 report by the U.K.'s Office for National Statistics found multifactor productivity in manufacturing firms increased 2.9 percent for every additional 10 percent of employees using Internet-enabled computers, compared with a 2.2 percent increase in productivity for each additional 10 percent of employees using computers. Similarly, productivity in services firms younger than the average for their sectors rose 1.7 percent for each 10 percent of employees using the Internet.[73] In addition, a 2009 analysis by representatives from 13 EU statistical offices found a positive relationship between labor productivity and employees having access to fast Internet in manufacturing. In addition, there was a strong association between productivity and the proportion of workers with access to high-speed Internet in the business and financial services industries in the Netherlands and United Kingdom.[74] Lastly, a 2009 Booz & Company analysis found that 10 percent higher broadband penetration correlated with 1.5 percent greater growth in labor productivity over the subsequent five years.[75]

Employment

Not only have numerous studies found a correlation between broadband penetration and employment, but others have also directly measured the number of jobs the Internet supports.[76] For example, in 2019, BEA conducted an analysis concerning the digital economy and found the U.S. digital economy had employed 5.1 million workers (3.3 percent of total employment) in 2017. Moreover, digital-economy employees earned $132,000 on average in annual compensation, which was significantly higher than the national average of $69,000.[77] Lastly, between 2011 and 2016, digital-economy employment grew at an average yearly rate of 3.7 percent, outpacing employment growth in the overall economy, which grew by only 1.7 percent.[78]

Innovation

A more open Internet increases innovation in multiple ways, including through better access to websites that provide self-learning opportunities (e.g., YouTube), more funding, and a greater spread of ideas through reduced communication costs.[79] Open technical standards also prevent

innovators from having to start from square one. For example, a person creating an Internet app does not need to create their own network, but rather only the application that will use the network.[80] While it is difficult to connect openness to innovation quantitatively, some studies link the Internet to increased innovation. For example, an analysis of U.K. ICT use surveys and the Community Innovation Survey demonstrates a significant link between high-speed Internet connections and employees' ability to use ideas outside the firm to innovate.[81]

COSTS OF REDUCING THE OPENNESS OF THE INTERNET

One way to identify the benefits of Internet openness is to measure the costs of closed policies—and if lawmakers are to maximize the benefits of Internet openness, they will have to avoid creating policies or conditions that result in unnecessary "closedness." Governments engage in policies that make the Internet more closed for a variety of reasons, including protecting privacy, ensuring political control or quelling social unrest, and protecting domestic and incumbent industries. This section discusses Internet shutdowns, data localization policies, and content blocking policies. The examples provided can help countries understand the potential costs of policies that close the Internet—which policymakers can weigh against the potential benefits of their actions.

Shutdowns and Application Blockages

Governments shut down access to the Internet and specific Internet applications for many reasons, including to stop the spread of fake news and to protect telecommunications firms from competition with VoIP services. Sometimes governments shut down the Internet for political reasons, such as to quell antigovernment protests. In such instances, shutdowns can slow the flow of information regarding government wrongdoing.[82] Governments have also blocked Internet access in order to achieve well-meaning goals, such as limiting cheating on standardized tests. While possible, it is unlikely the economic costs of Internet shutdowns will stop authoritarian governments from limiting access in order to secure their power. It may be possible, however, to convince governments that are shutting down the Internet with well-meaning intentions that the costs of the shutdowns outweigh the benefits.

It may be possible to convince governments that are shutting down or otherwise limiting the Internet with well-meaning intentions that the costs of the shutdowns outweigh the benefits.

Several organizations have quantified the economic costs of Internet shutdowns and blockages, which can range from blocking access to certain mobile applications to cutting off access to the entire Internet. For example, Deloitte estimated that a shutdown of the Internet and all its services would cost well-connected nations nearly $24 million for every10 million inhabitants per day.[83] The Brookings Institution, ICRIER, and the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) have each created formulas to demonstrate the costs of Internet shutdowns.[84] While the formulas vary, they each use a nation's or region's GDP and level of connectedness or size of their digital economy to estimate the costs of shutdowns.[85] Brookings examined 81 Internet shutdowns and major Internet application blockages that occurred between July 1, 2015, and June 30, 2016, and found these disruptions cost at least $2.4 billion in GDP globally.[86] Similarly, ICRIER examined mobile and fixed-line Internet shutdowns in India between 2012 and 2017, finding 16,000 hours' worth of disruptions cost the nation's economy

$3 billion.[87] Finally, CIPESA found the 176 days of total Internet shutdowns between 2015 and 2017 in 8 different African nations cost $218 million.[88]

Two common ways governments engage in application blocks and shutdowns is by directing ISPs to temporarily block specific URLs, and to require providers to completely shut down their services.[89] The length of the shutdowns varies widely. Algeria, for example, has shut down mobile and fixed-line Internet access for as little as one hour.[90] In contrast, Cameroon blocked access to social media and messaging applications in its Anglophone region for a number of months in 2018.[91]

Policymakers should understand that even temporary Internet disruptions can have significant economic effects. Like electricity blackouts, these Internet disruptions reduce productivity and result in the loss of time-sensitive transactions. For example, shutdowns have caused businesses to lose contracts by preventing them from being able to pay their suppliers and maintain contact with their clients. As a result of lost contracts, businesses have had to fire employees.[92] Internet shutdowns also create inefficiencies. For example, shutdowns in African countries have forced individuals to travel across borders in order to send emails, costing them money and time in the process.[93] Shutdowns can also have social costs. For example, medical professionals rely on the Internet to order supplies, so shutdowns hamper their ability to overcome medicinal shortages and provide medicine to all the individuals who need it.[94] The following examples discuss the costs of three reasons governments engage in Internet shutdowns and application blocks: reduce cheating on school exams, prevent violent protests, and protect telecommunication operators.

Reduce Cheating on School Exams

In recent years, several countries have shut down portions of the Internet in order to minimize cheating on standardized tests. For example, in 2016, Algeria blocked access to Facebook and Twitter to stop students from cheating on high school exams and, according to the government, protect students from "phony" exam-question topics individuals had posted online.[95] Two years later, the government ordered telecom operators to shut down access to the Internet entirely for up to three hours a day during a week of national high school exams.[96] Algeria is not alone, however. Governments in Iraq, India, and Uganda have each disrupted Internet services—often to block access to leaked exam answers that appear online before the tests—over concerns about exam cheating.[97] While governments should attempt to reduce cheating on standardized exams, blocking access to Internet applications and shutting down the Internet entirely are overly blunt methods to solve the problem. Indeed, even shutting down the Internet for a couple of hours in only one region can cost a country millions of dollars in lost GDP. For example, ICRIER found that a 2012 five-hour mobile and fixed Internet shutdown in the region of Jammu and Kashmir, which has 12.5 million people, cost nearly $3 million in lost GDP.[98] Similarly, the Brookings Institute found that Algeria's decision to block access to Facebook and Twitter for 6 days in 2016 cost the nation more than $20 million in GDP.[99] Using the Brooking Institute's formula for calculating the costs of Internet shutdowns, Algeria's 2018 decision to shut down the Internet for between 11 and 13 hours over 6 days in order to combat cheating cost between $6 million and $7 million—assuming the Internet economy accounted for only 1 percent of Algeria's GDP that year.[100] These examples show that before shutting down the Internet for even well-intentioned purposes, policymakers should consider the economic costs and weigh them against their social benefits. Furthermore, policymakers should understand their options are often not Manichean. Indeed, nations can both reduce cheating and receive the economic benefits of an accessible Internet.

Limit Protests

One of the most frequent reasons governments block Internet access is to slow or prevent protests—particularly violent ones. In many of these cases, the goal of governments is to ensure or restore public order.[101] Indeed, a spokesperson for the Bharatiya Janata Party, one of India's two major political parties, stated that shutdowns are acceptable in cases "where rumor-mongering or motivated misinformation could lead to the incitement of violence."[102] There are numerous examples of governments shutting down the Internet in order to stop protests or the spread of violence. For example, in 2015, the government of Rajkot, a city in the Indian state of Gujarat, suspended mobile Internet services for 10 hours after a politician threatened to hold a protest at a cricket stadium in which India would be playing South Africa.[103] In addition, real-time network data revealed that Iraq shut down access to the Internet for roughly 75 percent of individuals in the country during anti-corruption protests in October 2019.[104] As with attempting to restrict cheating, shutting down Internet services in order to prevent or slow protests is economically costly. For example, India shut down mobile Internet services for more than a week in 2016 in the city of Rohtak in order to stop the spread of rumors that could have exacerbated street protests.[105] The Brookings Institute estimated that this shutdown cost India $190 million in GDP.[106]

Internet shutdowns and social media blocks are also an ineffective way for governments to prevent nonviolent protests. Indeed, research suggests Internet shutdowns and application blocks can actually cause protest participants to substitute nonviolent action that relies on effective communication and coordination for violent tactics.[107] For example, an analysis of network shutdowns in India, which include both the cutting off of access to the Internet and other telecommunication services, found riots increase in intensity over the first three days of a shutdown. This research suggests that, contrary to the goals of many governments, reducing Internet access does not quell violent unrest—and at worst, may intensify unrest.[108]

Protect Traditional Telecommunication Operators

Governments have also blocked Internet services in order to protect the revenue model of legacy telecommunications industries. For example, in 2016, Saudi Arabia banned applications that had voice and video calling functions because domestic telecom operators were losing revenue from individuals choosing to use the cheaper and often-free Internet-based communication services.[109] Similarly, Morocco's telecommunications firms blocked access to applications such as Skype, Facebook, and WhatsApp for roughly 10 months in 2016. The Moroccan government supported the ban, stating none of the VoIP services had the required licenses—which represented a policy for a more closed Internet, as these Internet apps should not require a license. Morocco's Telecommunications Regulatory National Agency only allows commercial exploitation of IP telephony service through licensed operators; however, Internet-calling applications are often free or relatively cheap.[110] Brookings estimated this disruption cost Morocco nearly $1.8 million per day.[111] Saudi Arabia and Morocco are not alone, however. Several nations, including Qatar, have strict licensing requirements that limit the number of VoIP services available to the public.[112]

Because these Internet-based applications are usually free, or at least cheaper than traditional telephone calls, the cost to consumers is usually negligible. There is, however, a cost to future innovation when any application that competes with government-backed telecommunications firms sees competition squelched. Governments should be encouraging more flexibility in pricing

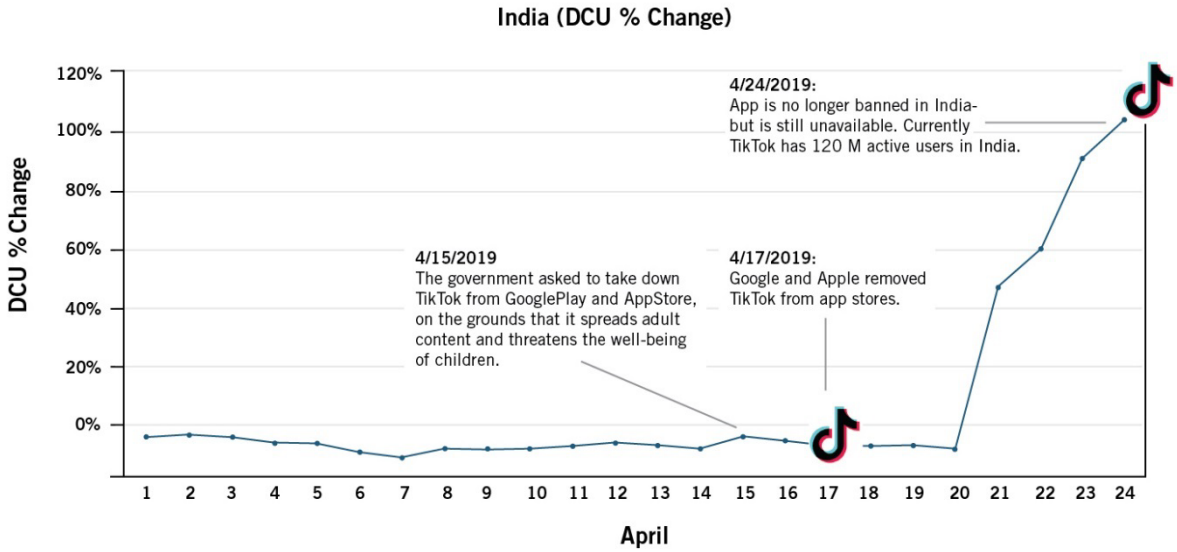
practices wherever necessary, more innovation around business models, and cooperative agreements between OTT and network providers that make both better off, to the ultimate benefit of consumers and businesses.

Blocking Popular Content

Many nations block the flow of data on the Internet that falls under the category of "universal bads," such as child pornography and the sale of drugs. Many nations also block access to content that falls under the category of "local bads"—content that some, but not all, nations find offensive enough to block. For example, India blocks access to certain pornographic websites in order to "protect social decency."[113] Some nations block access to content most other nations would not block, such as from independent media organizations. For example, between December 2018 and March 2019, Chinese authorities shut down more than 140,000 blogs and deleted more than 500,000 articles.[114] Blocking at this scale can have negative externalities, such as decreasing the value of the Internet for other nations. Internet blocking, for instance, can act as a trade barrier—the Office of the United States Trade Representative cited Chinese Internet blocking as a trade barrier in 2016.[115] It is difficult, however, to measure the cost of such blocking, both to the nation implementing the blocking and to other nations.

One way to begin understanding the value of a mostly open Internet and the costs of unnecessary content blocking is to analyze the growth in VPN use when governments block access to certain Internet-enabled services. While it is challenging to use growth in VPN use to place a precise value on a more open Internet, the decision of individuals to use a VPN in order to access blocked Internet services demonstrates the services have value. As a result, policies that block access to websites, applications, or VPNs reduce both the openness of the Internet and its value. High-level aggregate data obtained from Pango, an Internet privacy and security company that also offers a VPN service, allowed for the tracking of the increase in the number of daily connected users in countries in the days before and after bans of websites or mobile applications, which led to a better understanding of the value of certain Internet services.

Figure 2: Hotspot Shield VPN by Pango usage before and during India's ban of TikTok, April 15–24, 2019

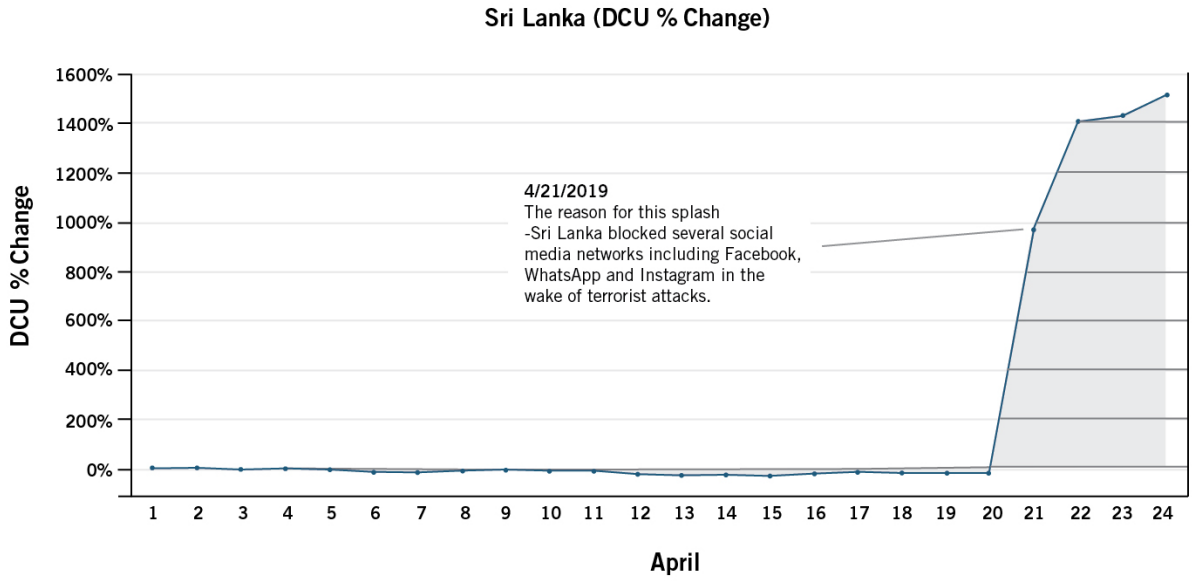


India Bans TikTok: On April 15, 2019, India's supreme court refused to stay the Madras High Court ban on TikTok, an app that allows users to create and share videos.[116] The court ruled that TikTok could expose minors to sexual predators, pornographic content, and cyberbullying.[117] Google and Apple subsequently removed the app from their respective app stores by April 17.[118] On April 24, the Indian court vacated its original order after TikTok appealed the decision, stating it had removed inappropriate content.[119] Between April 17 and 24, the number of individuals in India using Pango's VPN more than doubled.[120]

Sri Lanka Bans Social Media: On April 21, 2019, Sri Lanka banned the social media networks Facebook, WhatsApp, and Instagram for nine days in order to stop the spread of misinformation following terrorist attacks that killed or injured hundreds. Over the first four days of the ban, Pango's number of daily connected users more than tripled.[121]

While it is possible other variables besides bans could have caused that increases in the number of daily users, it is important to note Pango's number of daily users was relatively static in each of the preceding weeks. Consequently, these examples likely show that users, when faced with attempted blocks of Internet-enabled applications, value those applications enough to use a technical workaround. The surge in downloads of TikTok once the application was available again provides further evidence of the value of the application to users. It was the 90th most downloaded app in the Google Play Store in India the first day it was available following the ban, and the 15th most downloaded only a day later.[122]

Figure 3: Hotspot Shield VPN by Pango usage before and during Sri Lanka's ban of social media, April 21–30, 2019



Data Localization

International trade requires personal data—such as names, addresses, and billing information—be allowed to cross borders.[123] One of the primary benefits of a mostly openly Internet is its interconnected networks allow information to flow easily across borders, thereby increasing international trade. Indeed, a mostly open Internet makes it is easy for buyers and sellers to find each other online. Data localization policies, however, require firms to store and process data

domestically. Governments have implemented such policies for many reasons, including under the false belief data is more private and secure when firms store it within their nation. However, data localization can make personal data less secure by forcing firms to choose local providers that may not use best-in-class cybersecurity measures.[124] Nations have also required data localization policies under the false premise it would create a boom in data center jobs. In reality, data centers are highly automated, and therefore require only a small staff.[125]

Instead of increasing data security or creating jobs, data localization policies create myriad economic costs, including disrupting participation in global value chains and reducing economies of scale.[126] Multiple studies have shown data localization policies increase costs for local businesses. For example, a 2015 study by information-security company Leviathan found data localization policies would force local firms in many nations to pay 30 to 60 percent more for their computing needs. In particular, the study found businesses could save more than 36 percent on server costs by moving their servers outside the European Union.[127] In addition, a 2016 study from the Center for International Governance Innovation and Chatham House shows restrictive data regulations, including forced data localization, are likely to lead to increased prices and decreased productivity in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam.[128] Finally, data localization policies make it difficult for small businesses to sell their services and products globally because of the high cost of implementing separate systems for each nation that requires local data storage.[129]

A PRAGMATIC FRAMEWORK TO UNDERSTAND THE COSTS AND BENEFITS OF INTERNET OPENNESS

Policymakers need a framework to understand the benefits of Internet openness that is more nuanced than the conventional wisdom that "more is better." Indeed, calls for "no online censorship" and that "all Internet packets should be treated the same," or statements that "information wants to be free," imply policymakers should always pursue Internet openness as a goal in itself.[130] However, the relationship between an increase in Internet openness and the benefits of the Internet is not linear. For example, allowing child pornography online would technically increase the openness of the Internet. This level of openness, however, creates severe drawbacks. Moreover, some policies that reduce Internet openness, at least in the minds of hardcore net neutrality advocates, such as the prioritization of Internet traffic for first responders, are desirable.[131] Lastly, the social benefits of Internet openness can vary depending on each nation's different cultural values. For example, there are universal goods and bads, as well as local goods and bads.[132] A universal good related to Internet openness is an increase in trade. A universal bad is something most, if not all, nations would consider bad, such as the sale of widely banned drugs online. In contrast, a local good or bad is something wherein there is no international consensus. For example, some nations value freedom of speech more than do others and thus protect hate speech, thereby increasing freedom of expression and Internet openness—while countries such as Germany have made certain hate speech illegal.[133] In addition, some nations value privacy more than others. Certain elements of privacy regulations, such as the right to be forgotten, can reduce Internet openness and value. These differences in cultural values mean a framework that only tries to maximize openness cannot universally work.

A more useful framework is one that not only strives to make the Internet more open, but urges policymakers to pursue policies that maximize the benefits of Internet openness. Practically, this

goal equates to achieving a mostly open Internet by maximizing universal goods, reducing universal bads, and creating a high level of technical openness. At the architectural and protocol levels of the Internet, there is a need for commonly shared global standards to prevent the Internet from being balkanized.[134]

Policymakers will quickly learn that in most cases an increase in Internet openness simultaneously increases the economic and social benefits of the Internet, while closedness decreases both.

Nonetheless, many nations have also made international agreements. As a result, a framework for Internet policymaking first requires governments to consider whether their policies violate any agreements, regardless of how much they would benefit their nation. Next, to reduce policy conflicts between nations, governments should generally limit their policymaking activities to those that do not create negative impacts beyond their borders, particularly if there is no international consensus on a particular policy goal. For example, China's continued policy of not restricting online copyright infringement has a clear effect on the welfare of rights holders outside its borders. Consequently, even though this policy of acceptance increases Internet openness and provides its Internet users with access to free content, China should crack down on copyright infringement.[135] Finally, policymakers should determine whether policies increase or decrease the economic and social benefits of the Internet, and weigh them against the benefits of their policies. Policymakers will quickly learn that in most cases an increase in Internet openness simultaneously increases the economic and social benefits of the Internet, while closedness decreases both. For some policies, such as the sale of banned drugs, increasing Internet openness may bolster the economic value of the Internet (assuming it does not lead to households limiting Internet usage) but decrease its social value. Several policies and conditions that affect Internet openness provide further context and demonstrate how individuals can operationalize the framework.

Free Flow of Data

The existence of the World Trade Organization (WTO) is evidence of the international consensus that free trade is a universal good.[136] In addition, the relationship between the free flow of data—an element of Internet openness—and an increase an international trade in services is well documented. Moreover, the free flow of data facilitates Internet users' access to parts of the web that have social benefits, such as massive open online courses developed by organizations residing outside a user's nation. Finally, the purported benefits of polices that restrict data flows, such as data localization, are false (increased data security) or overblown (large increase in data center jobs). As a result, policymakers should support policies that increase the flow of data because it does not violate international agreements or negatively impact other nations—and increases the economic and social benefits the Internet provides. In contrast, policymakers should oppose policies such as data localization that not only reduce Internet openness but increase costs for local businesses. This should include opposing exemptions in digital trade agreements that allow nations to implement data localization as a means of protecting privacy.[137]

Internet Shutdowns and Application Blocks

In 2016 and 2018, the United Nations Human Rights Council passed resolutions stating disrupting Internet access is a human rights violation; however, the resolutions were non-binding.[138] Nonetheless, as this report and others have demonstrated, Internet shutdowns and

application blocks have tremendous costs. Many nations that pursue shutdowns do so for social reasons. For example, many nations have engaged in Internet shutdowns in order to stop the spread of false rumors, violence, and cheating on tests.[139] Policymakers should consider that even if shutdowns achieve their perceived goals, they also limit the social benefits of the Internet, including the ability of individuals to access information, express themselves online, and communicate with other individuals. Consequently, policymakers should not pursue Internet shutdowns, as they reduce both the economic and social value of the Internet.

Blocking Access to Legitimate Websites

Blocking legitimate websites clearly reduces Internet openness and the economic and social benefits the Internet provides—which alone should dissuade governments from such censorship. However, this argument may not be persuasive in nations that consider the blocked content to be a local bad, such as the lèse majesté laws in Thailand that forbid insulting the country's royalty.[140] Nonetheless, nations that engage in overly broad, indiscriminate website blocking may be in violation of their WTO commitments.[141]

While there is uncertainty, as many rules have never been subjects to a trade dispute, WTO rules require members to allow the unrestricted flow of cross-border Internet services due to the commitments they may have made under the General Agreement on Trade in Services (GATS).[142] However, there are numerous exemptions that raise considerable uncertainty about what is and isn't a legitimate restriction on data flows and the provision of cross-border services trade. For example, nations can block content, and therefore, the underlying data flows—which restricts the flow of cross-border Internet services—in order to protect public morals or maintain public safety.[143] But nations must prove their blocks are necessary to achieve their goals, and attempt to use less-trade-restrictive measures in order to reach their goals.[144] For example, China's decisions to block access to foreign news-organization websites such as *The New York Times*, *Bloomberg*, and *Wall Street Journal*—and not the web pages they think display objectionable content (whether for public morals, public safety, etc.)—are likely inconsistent with the provisions in GATS.[145] WTO members should initiate disputes that challenge such indiscriminate blocking, and ensure the new rules are developed to close loopholes nations use to justify broad data flow restrictions. Such a process would lead to the reduction of trade barriers and an increase in Internet openness.

Data Privacy Regulations

Governments have the right to create data privacy regulations, which can increase Internet openness by causing certain Internet users to have greater trust and engage in more activities online. However, there is little evidence to suggest that beyond some minimum baseline of consumer protection, stronger privacy regulations increase trust, adoption, or use.[146] Moreover, overly stringent privacy regulations can decrease Internet openness. For example, many individuals believe the European Union's General Data Protection Regulation (GDPR) provides social benefits by providing individuals with numerous rights online, including the right to request organizations delete their data.[147] In reality, the law has decreased Internet openness as some websites blocked European users, likely because of the law's high compliance costs. This list of organizations includes major media outlets such as *The Chicago Tribune* and *LA Times*.[148] Newspapers have also deleted articles in order to comply with the EU's right to be forgotten, which has been a privacy standard since 2014.[149] By limiting access to information, not only domestically but for Internet users outside the EU, the GDPR is hurting the social benefits of the

Internet. In addition, the law has had severe economic consequences, such as creating barriers to entry for start-ups due to high compliance costs, reduced competition in digital advertising, and reduced venture capital investment.[150] In this scenario, policymakers should consider ways to achieve their social goals that do not have significant economic and social drawbacks.

Blocking Access to Piracy Websites

Technically, any form of Internet blocking decreases Internet openness by limiting the websites users can access. Moreover, piracy websites often provide users access to cheap or free Internet content. Nonetheless, online piracy comes at the expense of content creators. For example, piracy costs the U.S. economy nearly $30 billion, and 230,000 jobs, annually.[151] More importantly, in regard to this framework, most nations that host piracy sites are members of the WTO and have signed multilateral agreements—such as the Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement—protecting intellectual property. Thus, while allowing piracy websites to exist increases Internet openness and possibly enhances the value the Internet provides, it has negative effects on the overall economy, and violates international agreements. As a result, policymakers should crack down on Internet piracy. To date, at least 42 countries have either adopted and implemented, or are legally obligated to adopt, measures ensuring ISPs block access to copyright-infringing websites.[152]

CONCLUSION

The Internet cannot maximize its potential economic and social benefits without a substantial amount of openness. But this does not mean nations should strive for complete openness; governments do and should limit access to universal bads. However, too many nations dress up restrictive internet policies as being in the public interest, when in fact they are in the interests of only a small set of powerful actors—and work against broader social and economic progress. As such, the goal of policymakers should be to maximize the benefits of Internet openness—while also implementing necessary guardrails—by blocking access only to bads that are universally agreed on, such as child pornography. This goal will ensure Internet users receive the vast benefits of the Internet without experiencing unnecessary harms.

About the Authors

Michael McLaughlin is a research analyst at the Center for Data Innovation and ITIF. He researches and writes about issues related to Internet policy, including digital platforms, e-government, and artificial intelligence. Michael graduated from Wake Forest University and received his Master's in Communication at Stanford University, specializing in Data Journalism.

Daniel Castro is vice president of ITIF and director of ITIF's Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow with Trust'" (Information Technology and Innovation Foundation, May 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust; Berhan Taye, "The State of Internet Shutdowns Around the World," Access Now, July 2019, https://www.accessnow.org/cms/assets/uploads/2019/06/KIO-Report-final.pdf; Sara Fischer and Alison Snyder, "A World and Web Divided," *Axios*, March 5, 2019, https://www.axios.com/internet-world-divided-5g-blockchain-4dcde946-d383-4b0c-89fb-64b21fee3730.html.

2. Berhan Taye, "The State of Internet Shutdowns Around the World."

3. "Russia Launches 'Disconnect From the Internet' Law," *CISO MAG,* November 4, 2019, https://www.cisomag.com/russia-launches-disconnect-from-the-internet-law/; Elizabeth Schulze, "Russia Just Brought in a Law to Try to Disconnect Its Internet From The Rest of the World," *CNBC*, November 1, 2019, https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html.

4. "Singapore: Reject Sweeping 'Fake News' Bill," Human Rights Watch, April 3, 2019, https://www.hrw.org/news/2019/04/03/singapore-reject-sweeping-fake-news-bill#; Ashley Westerman, "'Fake News' Law Goes Into Effect In Singapore, Worrying Free Speech Advocates," *NPR*, October 2, 2019, https://www.npr.org/2019/10/02/766399689/fake-news-law-goes-into-effect-in-singapore-worrying-free-speech-advocates; Ashley Westerman, "To The Dismay Of Free Speech Advocates, Vietnam Rolls Out Controversial Cyber Law," *NPR*, January 1, 2019, https://www.npr.org/2019/01/01/681373274/to-the-dismay-of-free-speech-advocates-vietnam-rolls-out-controversial-cyber-law.

5. Sara Fischer and Alison Snyder, "A World and Web Divided," *Axios*, March 5, 2019, https://www.axios.com/internet-world-divided-5g-blockchain-4dcde946-d383-4b0c-89fb-64b21fee3730.html; Berhan Taye, "The State of Internet Shutdowns Around the World."

6. Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India" (Stanford Global Digital Policy Incubator, February 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413; Daniel Kolitz, "What Would Happen If the Whole Internet Just Shut Down All of a Sudden," *Gizmodo*, August 19, 2019, https://gizmodo.com/what-would-happen-if-the-whole-internet-just-shut-down-1837346490; Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year" (Center for Technology Innovation at Brookings, October 2016), https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

7. Sarah Box and Jeremy West, *Economic and Social Benefits of Internet Openness* (Paris: Organization for Economic Development and Cooperation, June 2016), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En.

8. 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), http://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf.

9. Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), http://www2.itif.org/2018-trust-privacy.pdf.

10. Ellen Nakashima, "The U.S. Is Urging a No Vote on a Russian-Led U.N. Resolution Calling for a Global Cybercrime Treaty," *The Washington Post*, November 16, 2019, https://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11ea-818c-fcc65139e8c2_story.html; Shannon Vavra, "The U.N. Passed a Resolution That Gives Russia Greater Influence over Internet Norms," *CyberScoop*, November 18, 2019, https://www.cyberscoop.com/un-resolution-internet-cybercrime-global-norms/.

11. Elizabeth Economy, "The Great Firewall of China: Xi Jingping's Internet Shutdown," *The Guardian*, June 29, 2018, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

12. "Open Internet" (Digital Single Market, July 5, 2019), https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.

13. Sarah Box and Jeremy West, *Economic and Social Benefits of Internet Openness*.

14. Christina Warren, "How Do Computers Talk to Each Other on the Internet?" *Mashable*, October 17, 2012, https://mashable.com/2012/10/17/tcpip-faq/.

15. "Web Content Accessibility Guidelines (WCAG) 2.1" (World Wide Web Consortium), accessed September 10, 2019, https://www.w3.org/TR/WCAG21/; Sarah Box and Jeremy West, *Economic and Social Benefits of Internet Openness*.

16. Robert Atkinson, "Assessing the Costs of a More 'Closed' Internet" (Information Technology and Innovation Foundation, October 2, 2015), https://www.innovationfiles.org/assessing-the-costs-of-a-more-closed-internet.

17. Brad Plumer, "How easy is it to shut off a country's Internet?" *The Washington Post*, December 1, 2012, https://www.washingtonpost.com/news/wonk/wp/2012/12/01/how-easy-is-it-to-shut-off-a-countrys-internet/.

18. "Egypt Targets Social Media with New Law," Reuters, July 17, 2018, https://www.reuters.com/article/us-egypt-politics/egypt-targets-social-media-with-new-law-idUSKBN1K722C; Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism" (Freedom House, October 2018), https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

19. Robert Atkinson, "Assessing the Costs of a More 'Closed' Internet."

20. Sarah Box and Jeremy West, *Economic and Social Benefits of Internet Openness*.

21. As of November 2019, less than 30 percent of users accessed Google over IPv6; Google, Statistics (IPv6 Adoption, accessed November 17, 2019), https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption; Jennifer Bly, "Why is the Transition to IPv6 Taking So Long?" American Registry for Internet Users, August 13, 2014, https://teamarin.net/2014/08/13/transition-ipv6-taking-long/.

22. "DNS Attack," SearchSecurity, accessed September 12, 2019, https://searchsecurity.techtarget.com/definition/DNS-attack.

23. Chris Hoffman, "What is DNS Cache Poisoning?" *How-To Geek*, March 8, 2017, https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/.

24. See, Andrew Odlyzko, "Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation" (Digital Technology Center, University of Minnesota, 2004), http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf.

25. The Madison River case was easily resolved through consent decree in 2005, despite the lack of net neutrality rules. Madison River Communications, LLC and affiliated companies, File No. EB-05-IH-0110, Consent Decree, https://apps.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf.

26. See CyberTelecom, VoIP Blocking: Madison River - FCC VoIP Blocking Investigation 2005, https://www.cybertelecom.org/voip/blocking.htm.

27. ITU, "The Status of Voice Over Internet Protocol (VoIP) Worldwide, 2006" (2007), https://www.itu.int/osg/spu/ni/voice/papers/FoV-VoIP-Biggs-Draft.pdf.

28. Karl Flinders, "Skype Blocked in UAE Will Hit Businesses as Well as People," *Computer Weekly*, April 20, 2019, https://www.computerweekly.com/news/252461413/Skype-blocked-in-UAE-will-hit-businesses-as-well-as-people; Alvin Cabral, "Skype Blocked in UAE, but Here Are Some Other Alternatives," *Khaleej Times*, January 3, 2018, https://www.khaleejtimes.com/technology/skype-blocked-in-uae-but-here-are-some-other-

alternatives-; Saad Guerraoui, "Morocco Banned Skype, Viber, WhatsApp and Facebook Messenger. It Didn't Go down Well," *Middle East Eye*, March 9, 2016, https://www.middleeasteye.net/opinion/morocco-banned-skype-viber-whatsapp-and-facebook-messenger-it-didnt-go-down-well; Adrian Shahbaz, "Freedom on the Net 2016: Silencing the Messenger: Communication Apps Under Pressure."

29. ITU News, "New ITU Recommendation provides parameters for a collaborative framework for OTTs" (May 2019), https://news.itu.int/new-itu-recommendation-provides-parameters-for-a-collaborative-framework-for-otts/.

30. Damian Radcliffe, "Skype Banned, WhatsApp Blocked: What's Middle East's Problem with Messenger Apps?," *ZDNet*, December 11, 2017, https://www.zdnet.com/article/skype-banned-whatsapp-blocked-whats-middle-easts-problem-with-messenger-apps/.

31. Berhan Taye, "The State of Internet Shutdowns Around the World."

32. Software Freedom Law Center, Trends (Nature of Shutdown; accessed November 17, 2019), https://www.internetshutdowns.in.

33. Abdi Latif Dahir, "Chad Has Now Spent a Full Year Without Access to Social Media," *Quartz*, March 28, 2019, https://qz.com/africa/1582696/chad-has-blocked-whatsapp-facebook-twitter-for-a-year/; Bukola Adebayo, "After a 16-month Blackout, Chad is Back on Facebook, Twitter and Other Social Platforms," *CNN*, July 17, 2019, https://www.cnn.com/2019/07/17/africa/chad-restores-internet-intl/index.html.

34. Berhan Taye, "The State of Internet Shutdowns Around the World."

35. Ibid.

36. Bukola Adebayo, "After a 16-month Blackout, Chad is Back on Facebook, Twitter and Other Social Platforms," *CNN*, July 17, 2019, https://www.cnn.com/2019/07/17/africa/chad-restores-internet-intl/index.html.

37. "Chad - Where Social Media Has Been Cut for a Year," *BBC*, March 28, 2019, https://www.bbc.com/news/world-africa-47733383.

38. "Russia Internet: Law Introducing New Controls Comes into Force," *BBC*, November 1, 2019, https://www.bbc.com/news/world-europe-50259597; Andrei Soldatov, "Why Russia Might Shut Off the Internet," Foreign Affairs, March 29, 2019, https://www.foreignaffairs.com/articles/russian-federation/2019-03-29/why-russia-might-shut-internet.

39. Louise Matsakis, "What Happens if Russia Cuts Itself Off From the Internet," *Wired*, February 12, 2019, https://www.wired.com/story/russia-internet-disconnect-what-happens/.

40. Ibid.

41. "What is an Internet exchange point?" Cloudflare, accessed November 2, 2019, https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/.

42. Nick Harding, "Could the UK Government Shut down the Web?" *Independent*, March 8, 2011, https://www.independent.co.uk/life-style/gadgets-and-tech/features/could-the-uk-government-shut-down-the-web-2235116.html.

43. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

44. Nigel Cory, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored" (Information Technology and Innovation Foundation, April 1, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.

45. Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust'."

46. Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."

47. Javier C. Hernández, "Why China Silenced a Clickbait Queen in Its Battle for Information Control," New York Times, March 16, 2019, https://www.nytimes.com/2019/03/16/world/asia/china-bloggers-internet.html; Leng Shumei, "Beijing Shuts Down 110,000 Harmful Social Media Accounts," Global Times, December 26, 2018, http://www.globaltimes.cn/content/1133759.shtml; "WeChat Closes over 30,000 Accounts for Vulgar Content in 2019," Global Times, February 24, 2019, http://www.globaltimes.cn/content/1133759.shtml.

48. "The Internet, But Not as We Know It: Life Online in China, Cuba, India, and Russia," The Guardian, January 11, 2019, https://www.theguardian.com/technology/ng-interactive/2019/jan/11/the-internet-but-not-as-we-know-it-life-online-in-china-russia-cuba-and-india.

49. Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism."

50. Andrei Soldatov, "Why Russia Might Shut Off the Internet."

51. China's regulation states that individuals cannot receive a fine of more than 15,000 yuan ($2,100). In practice, fines appear to typically be around $150 (U.S.). See "Chinese Man Fined by Gov't for Trying to Access International Websites," *Inquirer.net*, January 7, 2019, https://technology.inquirer.net/82489/p2fb-chinese-man-fined-by-govt-for-trying-to-access-international-websites; Rob Mardisalu, "Are VPNs Legal In Your Country?" The Best VPN, last updated June 27, 2019, https://thebestvpn.com/are-vpns-legal-banned-countries/.

52. Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust'"; Claire Reilly, "AFP Using Site Blocking Laws to Target Malware," CNET, October 22, 2014, http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/; Nigel Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online" (Information Technology and Innovation Foundation, June12, 2018), https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online.

53. Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust'."

54. Ibid.

55. Freedom House, "Freedom on the Net 2019," Explore the Map, accessed November 18, 2019, https://www.freedomonthenet.org/explore-the-map.

56. Kevin Barefoot et al., "Research Spotlight Measuring the Digital Economy" (Washington, D.C.: U.S. Bureau of Economic Affairs, May 2019), https://apps.bea.gov/scb/2019/05-may/pdf/0519-digital-economy.pdf.

57. BEA used a supply-use framework to identify goods and services that are part of the digital economy. BEA uses the ICT sector as a starting point and includes digital-enabling infrastructure, e-commerce, and digital media as part of the digital economy. BEA only included goods and services from categories it deemed primarily digital in its digital economy estimates. Kevin Barefoot et al., "Research Spotlight Measuring the Digital Economy."

58. Ibid.

59. Ibid.

60. Ibid; "Defining and Measuring the Digital Economy" (Washington, D.C.: U.S. Bureau of Economic Affairs, May 2019), https://www.bea.gov/system/files/papers/WP2018-4.pdf.

61. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year"; Michael Minges, "Exploring the Relationship Between Broadband and Economic Growth" (World Bank, 2016), http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf.

62. Raji Kathuria et al., "Quantifying the Value of an Open Internet for India" (Indian Council for Research on International Economic Relations, July 2016), http://icrier.org/pdf/open_Internet.pdf.

63. Sarah Box and Jeremy West, *Economic and Social Benefits of Internet Openness.*

64. U.S. Bureau of Economic Analysis, International Data (International Transactions, International Services, and international Investment Position Tables, Table 3.1 U.S. Trade in ICT and Potentially ICT-Enabled Services, by Type of Service; accessed September 20, 2019), https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4.

65. Ibid.

66. Ibid.

67. George R. G. Clarke and Scott J. Wallsten, "Has the Internet Increased Trade? Evidence from Industrial and Developing Countries" (World Bank Policy Research Working Paper 3215, February 2004), http://documents.worldbank.org/curated/en/666781468778206389/108508322_20041117151016/additional/wps3215internet.pdf.

68. Behzad Salmani, Parviz Mohamadzadeh, and Maryam Saremi, "Internet and International Trade in Services," vol.5, no. 1 (2015): 212–220, https://www.researchgate.net/publication/271760737_Internet_and_International_Trade_in_Services.

69. "Micro-Multinationals, Global Consumers, and the WTO: Towards a 21st Century Trade Regime," (industry report, eBay Inc., 2013), www.ebaymainstreet.com/sites/default/files/Micro-Multinationals_Global-Consumers_WTO_Report_1.pdf; Sarah Box and Jeremy West, Economic and Social Benefits of Internet Openness.

70. Ibid.

71. Matthias Bauer et al, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" (European Centre for International Political Economy, 2013), https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf; Sarah Box and Jeremy West, Economic and Social Benefits of Internet Openness.

72. U.S. Department of Commerce, "Welcome to the Privacy Shield," accessed September 18, 2019, https://www.privacyshield.gov/welcome.

73. Tony Clayton, "IT Investment, ICT Use and UK Firm Productivity" (London: UK Office for National Statistics, August 2005), https://www.researchgate.net/profile/Raffaella_Sadun/publication/265671906_IT_Investment_ICT_Use_and_UK_Firm_Productivity/links/54b6907d0cf24eb34f6d2e98/IT-Investment-ICT-Use-and-UK-Firm-Productivity.pdf.

74. Mark Franklin, Peter Stam, and Tony Clayton, "ICT Impact Assessment by Linking Data," *Economic & Labour Market Review 3,* no. 10 (2009), https://link.springer.com/content/pdf/10.1057%2Felmr.2009.172.pdf.

75. Friedrich et al., "Digital Highways: The Role of Government in 21st-Century Infrastructure" (Booz & Company, 2009), http://www.strategyand.pwc.com/global/home/what_we_think/reports_and_white_papers/ic-display/46630268; Yongsoo Kim, Tim Kelly, and Siddhartha Raja, *Building Broadband: Strategies and Policies for the Developing World* (Washington, D.C.: The World Bank, 2010), 5.

76. Raji Kathuria et al., "Quantifying the Value of an Open Internet for India."

77. Kevin Barefoot et al., "Defining and Measuring the Digital Economy."

78. Ibid.

79. Raji Kathuria et al., "Quantifying the Value of an Open Internet for India."

80. Sarah Box and Jeremy West, Economic and Social Benefits of Internet Openness.

81. Mark Franklin, Peter Stam, and Tony Clayton, "ICT Impact Assessment by Linking Data."

82. Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," The New York Times, September 2, 2019, https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html.

83. "The Economic Impact of Disruption to Internet Connectivity" (Deloitte , October 2016), https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html.

84. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year"; Rajat Kathuria et al., "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India"; "The Economic Impact of Internet Disruptions in Sub-Saharan Africa" (Collaboration on International ICT Policy in East and Southern Africa, September 2017), https://cipesa.org/?wpfb_dl=252.

85. Ibid.

86. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year."

87. Rajat Kathuria et al., "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India."

88. "A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa" (Collaboration on International ICT Policy in East and Southern Africa, September 2017), https://cipesa.org/?wpfb_dl=252.

89. Christopher Giles, "Africa Internet: How do Governments Shut It Down?" BBC, March 31, 2019, https://www.bbc.com/news/world-africa-47734843.

90. Jon Henley, "Algeria Blocks Internet to Prevent Students Cheating During Exams," The Guardian, June 22, 2018, https://www.theguardian.com/world/2018/jun/21/algeria-shuts-internet-prevent-cheating-school-exams.

91. Yarno Ritzen, "Cameroon Internet Shutdowns Cost Anglophones Millions," Al Jazeera, January 26, 2018, https://www.aljazeera.com/news/2018/01/cameroon-internet-shutdowns-cost-anglophones-millions-180123202824701.html.

92. Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," The New York Times, September 2, 2019, https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html; "Policy Brief: Internet Shutdowns," Internet Society, November 13, 2017, https://www.internetsociety.org/policybriefs/internet-shutdowns#_edn20.

93. Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards."

94. Ibid.

95. Andrew Griffin, "Algeria Bans Facebook and Twitter in an Attempt to Stop People Cheating on Exams," Independent, June 20, 2016, https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-twitter-banned-blocked-algeria-exams-3g-internet-a7091171.html.

96. Jon Henley, "Algeria Blocks Internet to Prevent Students Cheating During Exams."

97. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year"; F. Brinley Bruton, "Iraq Blocks Internet to Stop Widespread Exam Cheating," NBC News, May 17, 2016, https://www.nbcnews.com/tech/social-media/iraq-blocks-internet-stop-widespread-exam-cheating-n575236.

98. Rajat Kathuria et al., "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India."

99. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year."

100. We used Brookings' national Internet shutdown costs formula to make this estimate. We multiplied Algeria's 2018 GDP ($180 billion), the duration of the shutdown as a percent of the year based on the number of days the Internet was shutdown (0.001256 or 0.001484), by the estimated extent of Algeria's digital economy (.01), and the multiplier effect (2.54) to get between roughly $6–7 million. We chose to conservatively estimate the Internet economy contributed 1 percent to Algeria's GDP in 2018. This estimation is lower than Boston Consulting Group's estimates for the percent the Internet economy contributed to any G20 nation's GDP in 2016. BCG estimated Indonesia's digital economy accounted for 1.5 percent of its GDP, for example. See Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year"; Jon Henley, "Algeria Blocks Internet to Prevent Students Cheating During Exams"; Rory Smith, "Algeria Turns Off Its Internet to Keep Students From Cheating On Exams," CNN, June 21, 2018, https://www.cnn.com/2018/06/21/africa/algeria-turns-off-internet-intl/index.html; David Dean et al., "The Connect World: The Internet Economy in the G-20" (industry report, Boston Consulting Group, March 2012), http://image-src.bcg.com/Images/The_Internet_Economy_G-20_tcm9-106842.pdf; World Bank, Data (Algeria, GDP (current US$; accessed November 18, 2019), https://data.worldbank.org/country/algeria.

101. Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India" (working paper, Global Digital Policy Incubator, Stanford University, February 7, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413.

102. Rahul Bhatia, "Growing Unease as India Curbs the net to Keep the Peace," LiveMint , September 18, 2017, https://www.livemint.com/Politics/t13L9GsLYgMHzoXZNj7L6J/Growing-unease-as-India-curbs-the-net-to-keep-the-peace.html; Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India."

103. Gopal Kateshiya, "Mobile Internet Services Banned in Rajkot as Patidar Threat Looms," The Indian Express, October 18, 2019, http://indianexpress.com/article/india/india-news-india/mobile-internet-services-banned-in-rajkot-as-patidar-threat-looms/.

104. Rae Hodge, "75% of Iraq's Internet Shut Down Amid Mass Protests," CNet, October 3, 2019, https://www.cnet.com/news/75-of-iraqs-internet-shut-down-amid-mass-protests/.

105. "Jat Reservation Protest in Haryana: Mobile Internet Services Blocked in Rohtak," India Today , February 19, 2016, https://www.indiatoday.in/india/story/jat-reservation-protest-in-haryana-mobile-internet-services-blocked-in-rohtak-309472-2016-02-18.

106. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year."

107. Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India."

108. Ibid.

109. "After WhatsApp, Facebook Messenger Gets banned in Saudi Arabia," Deccan Chronicle, May 17, 2016, https://www.deccanchronicle.com/technology/mobiles-and-tabs/170516/after-whatsapp-facebook-messenger-gets-banned-in-saudi-arabia.html; Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India."

110. Saad Guerraoui, "Morocco Banned Skype, Viber, WhatsApp and Facebook Messenger. It Didn't Go Down Well"; "You Can Make Skype Calls in Morocco Again," Fortune, November 4, 2019, https://fortune.com/2016/11/04/morocco-skype-ban/.

111. Darrell M. West, "Internet Shutdowns Cost Countries $2.4 Billion Last Year."

112. "Middle East Telecommunications & VOIP Challenges," Istizada, accessed November 1, 2019, http://istizada.com/blog/telecommunication-voip-challenges-in-the-middle-east/.

113. "Banned: Complete List of 857 Porn Websites Blocked in India," Deccan Chronicle, updated January 10, 2016, http://www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india.

114. Javier C. Hernández, "Why China Silenced a Clickbait Queen in Its Battle for Information Control," The New York Times, March 16, 2019, https://www.nytimes.com/2019/03/16/world/asia/china-bloggers-internet.html.

115. Tim Wu, "China's Online Censorship Stifles Trade, Too," The New York Times, February 4, 2019, https://www.nytimes.com/2019/02/04/opinion/china-censorship-internet.html.

116. Kuwar Singh, "A Time of How Things Went Downhill For TikTok In India," Quartz, April 17, 2019; https://qz.com/india/1598153/heres-why-tiktok-is-getting-banned-in-india/.

117. Rishi Iyengar, "India's Two-Week Ban Cost TikTok 15 Million Users," CNN, May 2, 2019, https://www.cnn.com/2019/05/02/tech/tiktok-ban-india-users/index.html.

118. "TikTok: Apple and Google Block Video Sharing App in India," BBC, April 17, 2019, https://www.bbc.com/news/business-47957684.

119. Aria Thaker, "An Indian Court Lifts the Ban on Downloading TikTok," Quartz, April 24, 2019, https://qz.com/india/1602417/tiktok-download-ban-lifted-by-indias-madras-high-court/.

120. Pango provided ITIF data on the number of their daily connected users for the VPN from April 1–April 24, 2019.

121. Ibid.

122. TikTok was offering users who downloaded the app a chance to win $1,400, which may have helped cause the surge in downloads. Aria Thaker, "TikTok is Regaining Its Position in India by Paying Indians to Download the App," https://qz.com/india/1610408/downloads-surge-as-tiktok-logo-returns-to-google-apple-in-india/.

123. Nigel Cory, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored" (Information Technology and Innovation Foundation, April 1, 2019), https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where; National Board of Trade Sweden, "No Transfer, No Trade—the Importance of Cross-Border Data Transfers for Companies Based in Sweden" (Stockholm, Sweden: National Board of Trade Sweden, January 2014), http://unctad.org/meetings/en/Contribution/dtl_ict4d2016c01_Kommerskollegium_en.pdf.

124. Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust'."

125. Nigel Cory, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored"; Grant Gross, "This Wave of Data Center Consolidation is Different from the First One" (Data Center Knowledge, February 8, 2018), https://www.datacenterknowledge.com/manage/wave-data-center-consolidation-different-first-one.

126. Sarah Box and Jeremy West, Economic and Social Benefits of Internet Openness.

127. Brendan O'Connor, "Quantifying the Cost of Forced Localization" (Leviathan Security Group, June 2015), http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization.

128. As part of the proxy variable for data regulations, the study uses part of the OECD's Product Market Regulation in services to create a proxy that comes close to matching the types of regulations that are used regarding data. The real policy regulations for the select countries are then added to this index to estimate the real costs. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization" (Centre for International Governance Innovation and Chatham House, May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf; Nigel Cory, "The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored."

129 . Jessica Nicholson and Ryan Noonan, "Digital Economy and Cross-Border Trade: the Value of Digitally-Deliverable Services" (Washington, D.C.: U.S. Department of Commerce, January 27, 2014), https://www.commerce.gov/sites/default/files/migrated/reports/digitaleconomyandcross-bordertrade.pdf; Sarah Box and Jeremy West, Economic and Social Benefits of Internet Openness.

130. Christopher Painter, Daniel Sepulveda, and Uzra Zeya, "Internet Freedom for All," *DipNote*, U.S. Department of State, August 13, 2013, http://blogs.state.gov/stories/2013/08/13/internet-freedom-all; "Say No To Online Censorship," Electronic Frontier Foundation, accessed July 8, 2014, https://www.eff.org/pages/say-no-to-online-censorship; Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014,), http://www2.itif.org/2014-crossborder-internet-policy.pdf.

131. Doug Brake, "Open Internet Oral Argument—Still Need a Bill" (Information Technology and Innovation Foundation, February 1, 2019), https://itif.org/publications/2019/02/01/open-internet-oral-argument-still-need-bill.

132. Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy."

133. "Germany: Dozens of Raids Over Online Hate Speech," Deutsche Welle, accessed November 21, 2019; https://www.dw.com/en/germany-dozens-of-raids-over-online-hate-speech/a-49080109.

126. Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy."

135. Ibid.

136. Ibid.

137. Nigel Cory, "EU Digital Trade Policy Proposal Opens a Loophole for Data Protectionism." *Euronews*, July 16, 2018, https://www.euronews.com/2018/07/16/eu-digital-trade-policy-proposal-opens-a-loophole-for-data-protectionism-view.

138. The Promotion, Protection, and Enjoyment of Human Rights on the Internet, United Nations General Assembly (Human Rights Council), 38th Session, Agenda Item 3, July 4, 2018, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement; Emma Flick, "UN Passes Resolution Condemning Internet Shutdowns," *ITPro*, July 3, 2016, https://www.itpro.co.uk/strategy/26843/un-passes-resolution-condemning-internet-shutdowns; "Saving the U.N. 'Internet Resolution' From Sharks Circling in Geneva," Access Now, July 10, 2018, https://www.accessnow.org/saving-the-u-n-internet-resolution-from-sharks-circling-in-geneva/.

139. Berhan Taye, "The State of Internet Shutdowns Around the World."

140. "Lese-Majeste Explained: How Thailand Forbids Insult of Its Royalty," *BBC*, October 6, 2017, https://www.bbc.com/news/world-asia-29628191.

141. For a comprehensive reading on the potential issues of such a WTO case, see Frederik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law" (European Centre for International Political Economy, 2009), http://ecipe.org/app/uploads/2014/12/protectionism-online-internet-censorship-and-international-tradelaw.pdf; Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost."

142. See Frederik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law"; "General Agreement on Trade in Services," World Trade Organization, accessed September 13, 2019, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

143. Ibid.

144. Frederik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law"; Claude Barfield, "Crafting an Action-Driven Response to China's Digital Trade Barriers" (American Enterprise Institute, January 2017), https://www.aei.org/wpcontent/uploads/2017/01/Crafting-an-action-driven-response-to-Chinas-digital-trade-barriers.pdf; "General Agreement on Trade in Services," World Trade Organization.

145. "The Complete List of Blocked Websites in China & How to Access them," VPNMentor, accessed November 21, 2019, https://www.vpnmentor.com/blog/the-complete-list-of-blocked-websites-in-china-how-to-access-them/; Craig Smith, "The New York Times vs. the 'Great Firewall' of China," *The New York Times*, March 31, 2017, https://www.nytimes.com/2017/03/31/insider/the-new-york-times-vs-the-great-firewall-of-china.html; "China to Lift ban on State-Owned Firms Buying Bloomberg Terminals, Source Says," *South China Morning Post*, September 6, 2017, https://www.scmp.com/news/china/diplomacy-defence/article/2015970/china-lift-ban-state-owned-firms-buying-bloomberg; Frederik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law."

146. Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), accessed October 9, 2018, http://www2.itif.org/2018-trust-privacy.pdf.

147. Barry Scott, "What's in It For Consumes? The Top 5 Privacy Benefits of the GDPR," *Centrify*, May 30, 2018, https://www.centrify.com/blog/consumer-privacy-benefits-gdpr/.

148. As of August 2018, both the *Chicago Tribune* and *LA Times* were unavailable in the European Union. Steve Dent, "Major US News Sites Are Still Blocking Europeans Due to GDPR," *Engadget*, August 9, 2019, https://www.engadget.com/2018/08/09/us-news-sites-unavailable-europe-gdpr/.

149. Adam Satariano, "Europe Is Reining In Tech Giants. But Some Says It's Going Too Far," *The New York Times*, May 6, 2019, https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html.

150. Eline Chivot and Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year" (Center for Data Innovation, June 17, 2019), https://itif.org/publications/2019/06/17/what-evidence-shows-about-impact-gdpr-after-one-year; Alec Stapp, "GDPR After One Year: Costs and Unintended Consequences," *Truth on the Market*, May 24, 2019, https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/.

151. James Pearce, "Digital Piracy Costs US Economy $30bn Annually" (IBC, July 1, 2019), https://www.ibc.org/consume/digital-piracy-costs-us-economy-30bn-annually/4037.article.

152. Nigel Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online" (Information Technology and Innovation Foundation, June12, 2018), https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online; Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust'."