



Computer & Communications  
Industry Association  
Tech Advocacy Since 1972

July 21, 2021

Ms. Lisa R. Barton  
Secretary to the Commission  
U.S. International Trade Commission  
500 E Street SW  
Washington, D.C. 20436

**Re: Investigation No. 332-585**

Dear Ms. Barton:

Pursuant to the notice issued by the U.S. International Trade Commission (ITC), the Computer & Communications Industry Association (CCIA) submits the following written comments in relation to Investigation No. 332-585: *Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses*.

These comments supplement the testimony delivered at the July 1, 2021 public hearing.

Respectfully submitted,

/s/ Rachael Stelly

Rachael Stelly  
Policy Counsel  
Computer & Communications Industry Association  
25 Massachusetts Avenue NW, Suite 300C  
Washington, DC 20001  
rstelly@ccianet.org  
Office: (202) 534-3901

*Before the*  
**Office of the United States International Trade Commission**  
Washington, D.C.

*In re*

**Foreign Censorship Part 1: Policies and  
Practices Affecting U.S. Businesses**

**Investigation No. 332-585**

**WRITTEN COMMENTS OF THE  
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)**

Pursuant to the notice issued by the U.S. International Trade Commission (ITC), the Computer & Communications Industry Association (CCIA) submits the following written comments in relation to Investigation No. 332-585: *Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses*.<sup>1</sup> CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.<sup>2</sup> CCIA welcomes the opportunity to document various regulations and policy frameworks that serve as market access barriers for Internet services.

**I. INTRODUCTION**

CCIA has long viewed foreign censorship of U.S. Internet services as having an international trade dimension, and is encouraged to see policymakers and the ITC devote resources to studying this topic and its impact on U.S. firms. The U.S. technology sector is on the front lines worldwide in the battle against government censoring, filtering, and blocking of Internet content. Many U.S. companies publish transparency reports that detail increased cases of Internet service disruptions, government requests for data, and content takedowns.<sup>3</sup> For

---

<sup>1</sup> This written submission supplements the oral testimony given at the July 1, 2021 public hearing in relation to Investigation No. 332-585: *Foreign Censorship Part 1: Policies and Practices Affecting U.S. Businesses* and Investigation No. 332-586: *Foreign Censorship Part 2: Trade and Economic Effects on U.S. Businesses*.

<sup>2</sup> For more, visit [www.cciagnet.org](http://www.cciagnet.org).

<sup>3</sup> See, e.g., Google Transparency Report, Traffic and Disruptions to Google, <https://transparencyreport.google.com/traffic/overview>; Government Requests to Remove Content, <https://transparencyreport.google.com/government-removals/overview> (last visited July 21, 2021); Twitter

example according to its transparency reports, Facebook notes that its services were interrupted 84 times in 19 countries in the second half of last year, compared to 52 disruptions in eight countries that took place during the first half of the year.<sup>4</sup> Just last month, Nigeria announced an “indefinite ban” on Twitter in the country following the company’s decision to remove posts from political leaders that violated its abusive behavior policy.

Censorship and denial of market access for foreign Internet services has long been the case in restrictive markets like China, but it is becoming increasingly common in emerging digital markets as well as some traditional large trading partners, and accomplished through using different tools and methods. Because the business community has a limited technical capacity to assess and respond to interference with cross-border flow of services, products, and information by nation-states, allied governments have a critical role to play in partnering with technology companies and leading in the defense of Internet freedom and open digital trade principles. However, to tackle these urgent issues, identification of key barriers is critical.

Government-imposed censorship of digital services and content takes multiple forms, and the risks associated with each method or regulatory framework providing for censorship methods can vary greatly. For example, some types of content restrictions may be reasonable and legally permissible in certain contexts, but may result in overbroad removals of user speech if attached to filtering or monitoring requirements. Other trade concerns arise where content policies are not applied equally to both domestic and foreign websites. Furthermore, an increasing number of content restrictions do not comply with World Trade Organization (WTO) principles of transparency, necessity, minimal restrictiveness, and due process to affected parties.

These comments: first, generally describe methods of censorship practices including certain regulations that can have the effect of censorship; second, identify certain trade rules that could be used to constrain foreign censorship; and third, provide a survey of foreign government practices that implicate censorship concerns.

---

Transparency Removal Requests Report, <https://transparency.twitter.com/en/reports/removal-requests.html#2020-jul-dec> (published July 14, 2021).

<sup>4</sup> *Facebook Says Government Internet Shutdowns Are on the Rise*, AXIOS (May 20, 2021), <https://www.axios.com/facebook-government-internet-shutdowns-censorship-a1c1c181-dc01-4450-9945-e1465f5139e8.html>.

## II. TYPES OF CENSORSHIP

### A. *Censorship and Internet Shutdowns*

Among the most explicit barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content, a trend that continues to grow. As the Washington Post Editorial Board observed in 2019, more governments are shutting down the Internet with disastrous consequences.<sup>5</sup> Access Now documented over 50 Internet shutdowns in 21 countries just in the first five months of 2021.<sup>6</sup> Internet shutdowns are also costly,<sup>7</sup> with one study finding that countries lose \$23.6 million (per 10 million in population) for every day that the Internet is shut down.<sup>8</sup> Despite these costs, governments continue to filter and block Internet content, platforms, and services for various reasons. For example, Iran has completely shut off access to the Internet in response to protests in the past.<sup>9</sup> And as discussed further below, the services of many U.S. Internet platforms are currently either blocked or severely restricted in the world's largest online market: China.

Whether deliberate actions to stifle political dissent or not, these practices clearly have trade-distorting effects well beyond the services directly involved. When a social media or video platform is blocked, it is not only harmful to the service and users in question, but it also immediately affects content providers, advertisers, and small businesses using the service to find and interact with new and existing customers. A Brookings Institution study estimated the global loss of intermittent blackouts at no less than \$2.4 billion in one year.<sup>10</sup> Such blocking is likely to violate international commitments, such as the World Trade Organization's rules on market access and national treatment.

---

<sup>5</sup> *More Governments Are Shutting Down the Internet. The Harm is Far-reaching*, WASH. POST (Sept. 7, 2019), [https://www.washingtonpost.com/opinions/more-governments-are-shutting-down-the-internet-the-harm-is-far-reaching/2019/09/06/ace6f200-d018-11e9-8c1c-7c8ee785b855\\_story.html](https://www.washingtonpost.com/opinions/more-governments-are-shutting-down-the-internet-the-harm-is-far-reaching/2019/09/06/ace6f200-d018-11e9-8c1c-7c8ee785b855_story.html).

<sup>6</sup> ACCESS NOW, *#KeepItOn Update: Who Is Shutting Down the Internet in 2021*, <https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/>.

<sup>7</sup> CCIA provides citations to available studies on the costs of Internet shutdowns at the infrastructure level for context in Part I of the USITC investigation, and intends to provide further updated estimates in response to Part 2 of the investigation.

<sup>8</sup> DELOITTE, *The Economic Impact of Disruptions to Internet Connectivity, A Report for Facebook*, at 6 (Oct. 2016), <https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf>.

<sup>9</sup> *Internet Disrupted in Iran Amid Protests in Multiple Cities*, NET BLOCKS (Nov. 15, 2019), <https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b>.

<sup>10</sup> Darrell M. West, *Global Economy Loses Billions from Internet Shutdowns*, BROOKINGS INST. (Oct. 6, 2016), <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>.

Methods of filtering and blocking generally consist of (a) legal or regulatory obligations imposed upon intermediary services, (b) network-level blocking and/or filtering achieved through state control of or influence over communications infrastructure, or (c) technology mandates that either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology.<sup>11</sup> A similar barrier to cross-border data flows is gateway filtering. When countries operate national firewalls, all foreign websites and services must pass through “gateways.” Domestic Internet content, however, does not pass through the gateways to reach its own domestic market. This has the effect of systemically affecting the speed and quality of service of foreign websites and services vis-à-vis domestic Internet content.<sup>12</sup>

To circumvent censorship measures by governments, users may use tools like Virtual Private Networks (VPNs) to access the restricted content or services, change a Domain Name Service (DNS) provider, or use the Tor Browser (either to access a blocked website or to protect a user’s identity).<sup>13</sup> In response to this, many countries where censorship is prevalent in turn restrict access to or criminalize use of VPNs. Countries that currently block or have restricted VPN use in the past include China, Iran, Russia, and Syria.<sup>14</sup>

### ***B. Content Restrictions and Regulations***

U.S. firms face an increasingly hostile regulatory environment in a variety of international markets which impedes U.S. Internet companies of all sizes from expanding their services abroad. Some of these regulations are in pursuit of legitimate and valid goals to address illegal content online; however, some proposals are more expansive in scope and directly conflict with U.S. law and free expression values. For example, there is a concerning trend in recent years among authoritarian governments pursuing content regulations to fight “fake news”, which often go beyond standard efforts to remove disinformation and instead have the primary effect of

---

<sup>11</sup> WORLD ECONOMIC FORUM, *Internet Fragmentation: An Overview* at 35-36 (2016), [http://www3.weforum.org/docs/WEF\\_FII\\_Internet\\_Fragmentation\\_An\\_Overview\\_2016.pdf](http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf).

<sup>12</sup> Alexander Chipman Koty, *China’s Great Firewall: Business Implications*, CHINA BRIEFING (June 1, 2017), <https://www.china-briefing.com/news/chinas-great-firewall-implications-businesses/>.

<sup>13</sup> ELEC. FRONTIER FOUND. (EFF), *Understanding and Circumventing Network Censorship* (Apr. 2020), <https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship>.

<sup>14</sup> *Infra*, p. 14. See also VPN blocking, [https://en.wikipedia.org/wiki/VPN\\_blocking#Government\\_use](https://en.wikipedia.org/wiki/VPN_blocking#Government_use) (last visited July 21, 2021).

targeting dissidents and political opposition.<sup>15</sup> Separately, there are increasing foreign trends that require U.S. companies to:

- remove speech that may be legal within a country but that conflicts with vaguely defined norms about “harmful” content;
- adhere to broadly defined “duties of care” that require general monitoring of all user content posted to an Internet service;
- pre-install, give preferential treatment to, or provide data to foreign technology companies that may restrict speech or surveil users in a manner that conflicts with U.S. law and values;
- break encryption by enabling the “traceability” of originators of content; and
- designate local employees that will be subject to imprisonment in cases of non-compliance with a local content requirement.

Context and how certain rules are being enforced in a market are important when evaluating regulations pertaining to removal of online content and may determine risk of censorship and potential trade-distortive practices. For instance, the presence, or lack thereof, of legal norms such as due process may help reduce impact for U.S. firms operating abroad. It is important that good regulatory practices are followed as governments consider new rules on addressing harmful and illegal content; are designed to limit unintended consequences, especially those that impact online speech; and are compliant with trade commitments.

To be clear, an increasing number of Internet services recognize the importance of ensuring user trust and safety in their platforms and have significantly increased resources to ensure that their services remain spaces for free expression, that users comply with their terms of service, and that illegal and harmful content that violates their terms of service is identified and removed from their platform. But the expanding array of censorship obligations described in these comments often have the impact of making it harder, rather than easier, for U.S. Internet companies to strike the right balance between promoting free expression and taking action against illegal content.

---

<sup>15</sup> *The Rise of Digital Authoritarianism: Fake News, Data Collection and the Challenge to Democracy*, FREEDOM HOUSE (Oct. 2018), <https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy> (“Citing fake news, governments curb online dissent: At least 17 countries approved or proposed laws that would restrict online media in the name of fighting “fake news” and online manipulation. Thirteen countries prosecuted citizens for spreading allegedly false information.”).

### III. CONFLICTS WITH INTERNATIONAL TRADE OBLIGATIONS

Restrictions on Internet content and services may be prohibited by both the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS), as noted in the previous section.<sup>16</sup>

With respect to GATT obligations, while the function of GATT governs trade in physical goods, there is the possibility for the application of these commitments in the digital context. It is certainly the case that online services which implicate neither downloaded nor stored goods, such as search and social media, must be considered “services,” analyzed with reference to GATS, not GATT. Nevertheless, disagreements remain regarding products that are downloaded, and kept in digital form, “like newspapers, songs, software, audio, and electronic books. While the WTO has yet to rule on the issue, the better position is that the digital versions of goods remain ‘goods’ subject to GATT.”<sup>17</sup> In any event, physical goods may be purchased through digital means, and thereby implicating the objectives embodied in GATT. GATT requires a contracting party to afford goods supplied from abroad similar status to like products originating from domestic suppliers.<sup>18</sup> Yet in many cases platforms and services through which digital products can be obtained are subjected to specific censorship that provides a competitive advantage to similar products originating in China. Certain U.S. social media services, for example, have been completely blocked in China, while their Chinese equivalents Weibo and Renren are allowed to operate with selective filtering. GATT similarly requires “[l]aws, regulations, judicial decisions and administrative rulings of general application” to be published promptly, and to be administered in a “uniform, impartial and reasonable manner.”<sup>19</sup> The filtering, blocking, and censorship that U.S. services encounter, however, generally remains unpublished and unevenly applied. Moreover, little legal recourse exists to dispute the administration of such measures.

With respect to GATS, numerous provisions of GATS prohibit the filtering, blocking, and censorship that is applied to Internet services. GATS imposes considerable obligations on

---

<sup>16</sup> CCIA Testimony Before U.S.-China Economic and Security Review Commission, “Commercial Espionage and Barriers to Digital Trade in China”, June 15, 2015, *available at* <https://www.ccianet.org/wp-content/uploads/2015/06/Barriers-to-Digital-Trade-in-China-Testimony-6.15.15.pdf> [“2015 CCIA Testimony Before U.S.-China Economic and Security Review Commission”].

<sup>17</sup> Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 Chi. J. Int’l L. 263, 268 (2006).

<sup>18</sup> GATT Art. III:4 (1947 text).

<sup>19</sup> GATT Arts. X:1, X:3(a)-(b).

WTO Members, mandating transparency, impartiality, and nondiscrimination in trade-related government actions, and requires that affected parties be afforded opportunities for judicial or independent review of trade-related administrative decisions. While exceptions to these obligations exist, such as for “public morals”/“public order”,<sup>20</sup> GATS derogations are only permissible when necessary to achieve the stated objective, where no reasonable, less restrictive alternative exists, and when applied without prejudice.<sup>21</sup> Where nations implement filtering, blocking, and censoring of online services, these standards are rarely met. It is necessary to note that whereas GATT imposes blanket commitments, GATS governs sectors and “modes” where a contracting party has made specific commitments. The Chinese Government has made specific commitments pertaining to various web-based service sectors, however, as well as value-added telecommunications.<sup>22</sup> As with GATT, GATS requires reasonable publication and impartial administration of trade related regulatory measures. When U.S. services encounter arbitrary restrictions, often at odds with what domestic competitors are subjected to, it likely constitutes a GATS violation.<sup>23</sup> The market access commitments contained in GATS Article XVI also apply in this context.

#### **IV. SURVEY OF FOREIGN PRACTICES**

This section provides an overview of varying foreign censorship practices, as well as certain content-related restrictions that may have the effect of censoring and/or restricting lawful content online. This survey is not exhaustive of all censorship threats to U.S. firms, but rather illustrates both key regions of concern such as Turkey, India, and Russia, as well as illustrating different types of practices that pose content-related barriers to trade.

CCIA notes that the size of the impact to U.S. firms as well as the impact on free expression varies significantly across the regimes included in this submission. As noted above, context and how the regulation is being enforced is important when evaluating the risk of censorship in various content-based regulations.

---

<sup>20</sup> Exceptions for “public morals”/“public order” may be found in GATT Art. XX(a) and GATS Art. XIV(a).

<sup>21</sup> GATS Art. XIV. *See* Wu, *supra* note 17, at 272.

<sup>22</sup> Frederik Erixon, Brian Hindley, & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law* (2009), <https://www.ecipe.org/publications/protectionism-online-internet-censorship-and-international-trade-law/>.

<sup>23</sup> GATS Art. XVII:1.



## A. Australia

Australia amended its Criminal Code in April 2019 to establish new penalties for Internet and hosting services who fail to provide law enforcement authorities with details of “abhorrent violent material” within a reasonable time, or fail to “expeditiously” remove and cease hosting this material.<sup>24</sup> The Australian legislation illustrates the importance of following good regulatory practices with opportunities for all stakeholders to provide input into the legislative process when countries pursue regulations that affect online speech. Criticism was directed at the rushed nature of the drafting and legislative process.<sup>25</sup> The legislation applies to a broad range of technology and Internet services, including U.S.-based social media platforms, user-generated content and live streaming services, and hosting services. However, the law does not consider the varying business models of these services in the scope of the law and their varying capabilities or roles in facilitating user-generated content.

## B. Brazil

A law designed to address “fake news” was passed by the Senate in July 2020, the *Internet Freedom, Responsibility, and Transparency Bill*.<sup>26</sup> While there were improvements from its initial draft,<sup>27</sup> concerns remain including around ambiguity in key definitions<sup>28</sup> and the fear that some requirements would be used in a manner to pursue restrictions on speech.<sup>29</sup>

---

<sup>24</sup> Criminal Code Amendments (Sharing of Abhorrent Violent Material) Bill 2019, [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bId=s1201](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201).

<sup>25</sup> See Evelyn Douek, *Australia’s New Social Media Law Is a Mess*, LAWFARE (Apr. 10, 2019), <https://www.lawfareblog.com/australias-new-social-media-law-mess>.

<sup>26</sup> Available at <https://legis.senado.leg.br/sdleg-getter/documento?dm=8127649&ts=1593563111041&disposition=inline>.

<sup>27</sup> *Update on Brazil’s Fake News Bill: The Draft Approved by the Senate Continues to Jeopardize Users’ Rights*, CENTER FOR DEMOCRACY & TECHNOLOGY (July 24, 2020), <https://cdt.org/insights/update-on-brazils-fake-news-bill-the-draft-approved-by-the-senate-continues-to-jeopardize-users-rights/>; *Brazilian Senate Passes Fake News Bill*, ZDNet (July 1, 2020), <https://www.zdnet.com/article/brazilian-senate-passes-fake-news-bill/>

<sup>28</sup> *Brazil, Democracy, and the “Fake News” Bill*, GLOBAL AMERICAS (Jan. 4, 2021), <https://theglobalamericans.org/2021/01/brazil-democracy-and-the-fake-news-bill/> (“Whereas some people think that the bill proposes reasonable and necessary measures to combat disinformation, others worry that it could be misused as censorship. What is more, some also argued that, even if it were adopted, the problem of disinformation would not be solved because of the inherent difficulty in identifying and collectively agreeing on what is considered fake news. The definition employed in the bill is ambiguous, which enables the state to arbitrarily sort out what types of information might be deemed false or offensive. Moreover, the bill disregards a bigger issue: the users that further spread harmful content. Rather than directly approaching the responsible accounts disseminating false information, it aims to “discourage the use of inauthentic accounts.”).

<sup>29</sup> *Brazil’s Bolsonaro Would Veto Bill Regulating Fake News in Current Form*, REUTERS (July 2, 2020), <https://www.reuters.com/article/us-brazil-politics-fake-news-idUSKBN2433FN> (citing a joint statement by Facebook, Twitter and Google jointly criticizing the bill “as a serious threat to privacy”); *Brazil: Disinformation bill*

Further, the draft bill retains a traceability requirements for online messaging services and verification requirements for users that may post threats to the security of communications. Industry is also monitoring developments around a possible Executive Order that would penalize firms if they enforced terms of service regarding harmful content against political leaders.

### **C. Cambodia**

Reports of censorship and mandated Internet filtering and blocking continue to rise in Cambodia, with recent cases reportedly directed at access to news sites in wake of the COVID-19 pandemic.<sup>30</sup> Legislation passed in April 2020 grants extensive authorities to the government to restrict information online if a state of emergency is imposed.<sup>31</sup>

### **D. China**

China has long been a region of concern for U.S. Internet services.<sup>32</sup> China has implemented various techniques not only against foreign websites, known aptly as the “Great Firewall of China,” but to a lesser extent domestically as well. Some have explained the elaborate Chinese censorship system as being geared towards maximizing the economic benefits of the Internet while maintaining strict social control. Whatever the domestic aim of these mechanisms may be, they function, intentionally or not, as unlawful barriers to international trade. For many years, U.S. sites, platforms and services have been intermittently or persistently blocked at the network level, often over relatively trivial content or for “dubious” reasons.<sup>33</sup> Chinese authorities have been known to redirect traffic from U.S.-based search engines to Baidu, their China-based competitor,<sup>34</sup> and Baidu’s share of the Chinese search market has increased. More recently, this discriminatory treatment escalated even further, with analytics traffic in China being redirected from Baidu at the network level toward U.S. sites as a form of malicious distributed denial of service (DDoS). Victims included GitHub, a platform popular among programmers, and the censorship-tracking site GreatFire, both of which provided tools that allow

---

*Threatens Freedom of Expression and Privacy Online*, FREEDOM HOUSE (June 2020), <https://freedomhouse.org/article/brazil-disinformation-bill-threatens-freedom-expression-and-privacy-online>.

<sup>30</sup> Freedom on the Net 2020: Cambodia (2020), available at <https://freedomhouse.org/country/cambodia/freedom-net/2020>.

<sup>31</sup> *Id.* at C1, The Law on the Management of the Nation in a State of Emergency.

<sup>32</sup> See 2015 CCLA Testimony Before U.S.-China Economic and Security Review Commission, *supra* note 16.

<sup>33</sup> See, e.g., Claudine Beaumont, *Foursquare Blocked in China*, THE TELEGRAPH (June 4, 2010), <https://www.telegraph.co.uk/technology/social-media/7802992/Foursquare-blocked-in-China.html>.

<sup>34</sup> John Biggs, *Cyberwar: China Declares War On Western Search Sites*, TECHCRUNCH (Oct. 18, 2007), <https://techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/>.

Chinese citizens to circumvent network-level censorship.<sup>35</sup> This event followed soon after Chinese authorities announced a new initiative to “guide Internet-based companies to increase their presence in the international market.”

While many U.S. Internet companies are effectively blocked from the Chinese market, their Chinese Internet competitors not only have access to U.S. markets, but rely on them to engage leading providers of financial, legal, and technical services, as well as U.S. hardware. It bears noting that while these strategies are practiced within China, they are also practiced by other nations as well, with the result being that U.S. services are allowed uneven and unequal access to numerous growing markets abroad.

### **E. Cuba**

There have been many cases of the Cuban government disrupting access or blocking certain Internet services to stifle political dissent and organization.<sup>36</sup> Government ownership and control of the *Empresa de Telecomunicaciones de Cuba S.A.*, the telecommunications services provider for the country, increases the risk of censorship. In response to political protests, Cuban authorities have blocked access to many U.S. social media platforms including Facebook, WhatsApp, and Twitter in November 2019, and most recently in July 2021.<sup>37</sup>

### **F. European Union**

In the European context, the risks of extraterritorial application of certain content related takedown requirements are evident.

The General Data Protection Regulation (GDPR) includes a “right to erasure” provision, which codifies the “right to be forgotten” and applies it to all data controllers. Under Article 17, controllers must erase personal data “without undue delay” if the data is no longer needed, the

---

<sup>35</sup> Russell Brandom, *China’s ‘Great Cannon’ Can Intercept and Redirect Web Traffic*, THE VERGE (Apr. 10, 2015), <https://www.theverge.com/2015/4/10/8381827/china-great-cannon-firewall-web-censorship>; Nicole Perlroth, *China Is Said to Use Powerful New Weapon to Censor Internet*, N.Y. TIMES (Apr. 10, 2015), <https://www.nytimes.com/2015/04/11/technology/china-is-said-to-use-powerful-new-weapon-to-censor-internet.html>.

<sup>36</sup> *Cuba’s Social Media Blackout Reflects an Alarming New Normal*, WIRED (July 13, 2021), <https://www.wired.com/story/cuba-social-media-blackout/>. (“Cuba’s national telecommunications company Etecsa, which offers both broadband and Cubacel mobile data, was founded in 1994. But the government historically has heavily restricted who could have an internet connection and only began slowly opening up access in 2016. In 2019 the regime first began allowing limited connections in private homes and businesses. The combination of total control and nascent user base makes it relatively easy for the government to carry out both widespread internet shutdowns and platform-specific blocking.”).

<sup>37</sup> *Id. Faced With Rare Protests, Cuba Curbs Social Media Access, Watchdog Says*, REUTERS (July 13, 2021), <https://www.reuters.com/world/americas/cuba-curbs-access-facebook-messaging-apps-amid-protests-internet-watchdog-2021-07-13/>.

data subject objects to the processing, or the processing was unlawful.<sup>38</sup> Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4 percent of a company's global operating costs. U.S. services have fielded hundreds of thousands of requests since the policy went into effect.<sup>39</sup> Processing these requests requires considerable resources because each request must be examined individually. Small and medium-sized enterprises that also offer similar services but without similar resources to field these requests could find that the "right to be forgotten" and "right to erasure" pose a barrier to entry into the EU.

In 2019, the Court of Justice of the European Union (CJEU) provided some parameters on the global enforcement of these requests. The CJEU declined to require the extraterritorial application of a removal request.<sup>40</sup> However, the opinion left open the option for extraterritorial application in certain cases.

The CJEU notes:

While EU law does not currently require a de-referencing to be carried out on all versions of the search engine, it also does not prohibit such a practice. Accordingly, the authorities of the Member States remain competent to weigh up, in the light of national standards of protection of fundamental rights, a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.<sup>41</sup>

This could lead to conflict of laws issues where a service provider may be required under EU law to remove content that is lawful elsewhere.

In the defamation context, the EU Court of Justice ruled in a 2019 case that host providers could be asked to take down defamatory content that is "identical" or "equivalent" to content previously ruled illegal under national rules.<sup>42</sup> The decision essentially allows one country or region to decide what Internet users around the world can say and what information

---

<sup>38</sup> GDPR art. 17.

<sup>39</sup> Alex Hern, *Google Takes Right to be Forgotten Battle to France's Highest Court*, THE GUARDIAN (May 19, 2016), <https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court>.

<sup>40</sup> Press Release No. 112/19, Judgment in Case C-507/17, 24 Sept. 2019, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf>.

<sup>41</sup> *Id.*

<sup>42</sup> Case C-18/18, 3 Oct. 2019, *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd.*, available at <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1967126>.

they can access, raising free expression concerns.<sup>43</sup>

### **G. France**

In March 2019, the National Assembly proposed a very broad law on combating hate speech (“*Lutte contre la haine sur internet*”).<sup>44</sup> The law would require designated Internet services to take down hateful comments reported by users within 24 hours. The law targeted any hateful attack on someone’s “dignity” on the basis of race, religion, sexual orientation, gender identity, or disability. Platforms face an administrative penalty of 4 percent of their global revenue and penalties could reach tens of millions of euros. The French National Assembly adopted the law on May 13, 2020. However, the French Constitutional Court released a decision pertaining to the constitutionality of the new law on June 18, 2020.<sup>45</sup> The Court determined the legislation “undermines freedom of expression and communication in a way that is not appropriate, necessary and proportionate to the aim pursued” making the text not compatible with the French constitution. The Court also struck down the one-hour removal deadline for terrorist propaganda and child pornographic contents as it contradicts the French Penal code (Art. 227-3 and 421-2-5).

### **H. Germany**

Germany adopted the Act to Improve the Enforcement of Rights on Social Networks (the “Network Enforcement Law” or “NetzDG”) in June 2017.<sup>46</sup> The NetzDG law mandates removal of “manifestly unlawful” content within 24 hours, and provides for penalties of up to 50 million euros.<sup>47</sup> Unlawful content under the law includes a wide range of content from hate speech to unlawful propaganda. The large fines and broad considerations of “manifestly unlawful content”<sup>48</sup> have led to companies removing lawful content, erring on the side of caution in

---

<sup>43</sup> See Statement of CCIA, EU Court Ruling on Worldwide Takes Down of Defamatory Content Raises Freedom of Speech Concerns (Oct. 3, 2019), *available at* <https://www.cciainet.org/2019/10/915157/>.

<sup>44</sup> *Lutte contre la haine sur internet*, Assemblée Nationale, [http://www.assembleenationale.fr/dyn/15/dossiers/lutte\\_contre\\_haine\\_internet](http://www.assembleenationale.fr/dyn/15/dossiers/lutte_contre_haine_internet).

<sup>45</sup> Conseil constitutionnel [CC] [Constitutional Court] decision No. 2020-801DC, June 18, 2020 (Fr.), *available at* <https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm>.

<sup>46</sup> Beschlussempfehlung und Bericht [Resolution and Report], Deutscher Bundestag: Drucksache [BT] 18/13013, <http://dip21.bundestag.de/dip21/btd/18/130/1813013.pdf> (Ger.). Unofficial English translation *available at* <https://medium.com/speech-privacy/what-might-germanys-new-hate-speech-take-down-law-meanfortechcompanies-c352efbbb993>.

<sup>47</sup> *Id.* § 3(2).

<sup>48</sup> The law is designed to only apply to social media companies (it was informally referred to as the ‘Facebook law’), but a wide variety of sources may also be implicated as the law is so broadly written to include sites that host third party content including Tumblr, Flickr, and Vimeo. Social media networks are defined as a tele-

attempts to comply.<sup>49</sup> Since coming into force in January 2018, the law has already led to high-profile cases of content removal and wrongful account suspensions. Companies have repeatedly raised concerns regarding the law’s specificity and transparency requirements<sup>50</sup> and groups have expressed concerns about its threats to free expression.<sup>51</sup>

This law is concerning to the extent it creates a potential domino effect of this policy on other regimes, and has been cited as the basis for several concerning content regulations including legislation in Russia, Singapore, Turkey, and Venezuela.<sup>52</sup> Cases arising under this law also implicate extraterritoriality concerns.<sup>53</sup>

## I. India

India is a priority region of concern for U.S. digital service exporters, given the vibrant digital economy and market opportunities and increased government control over online speech. There is great concern with the speed at which Indian policymakers and political leaders have increased censorship practices and increased restrictions on companies that fail to take down content political leaders deem “objectionable”. This has been combined with a dramatic increase

---

media service provider that operate online platforms (1) with the intent to make a profit, and (2) on which users can share content with other users or make that content publicly available. *See Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under “Facebook Act”*, LIBRARY OF CONGRESS (June 30, 2017), <https://www.loc.gov/item/global-legal-monitor/2017-07-11/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/>.

<sup>49</sup> CEPS, Germany’s NetzDG: A Key Test for Combatting Online Hate (2018), *available at* [https://www.ceps.eu/system/files/RR%20No2018-09\\_Germany%27s%20NetzDG.pdf](https://www.ceps.eu/system/files/RR%20No2018-09_Germany%27s%20NetzDG.pdf).

<sup>50</sup> Thomas Escritt, *Germany Fines Facebook for Under-Reporting Complaints*, REUTERS (July 2, 2019), <https://www.reuters.com/article/us-facebook-germany-fine/germany-fines-facebook-for-under-reporting-complaints-idUSKCN1TX11C>.

<sup>51</sup> *Germany: Flawed Social Media Law*, HUMAN RIGHTS WATCH (Feb. 14, 2018), <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law> (“[T]he law places the burden on companies that host third-party content to make difficult determinations of when user speech violates the law, under conditions that encourage suppression of arguably lawful speech. Even courts can find these determinations challenging, as they require a nuanced understanding of context, culture, and law. Faced with short review periods and the risk of steep fines, companies have little incentive to err on the side of free expression.”).

<sup>52</sup> Jacob Mchangama & Natalie Alkiviadou, *The Digital Berlin Wall: How Germany Built a Prototype for Online Censorship*, EURACTIV (Oct. 8, 2020), <https://www.euractiv.com/section/digital/opinion/the-digital-berlinwall-how-germany-built-a-prototype-for-online-censorship/>.

<sup>53</sup> *See* INTERNET SOCIETY, *The Internet and Extra-Territorial Effects of Laws* (Sept. 2018), *available at* <https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws-EN.pdf> at 17-18 (“the law applies to any platform, regardless of whether it would ordinarily fall within German jurisdiction, where hate speech may be uploaded or viewed by a German citizen or resident. Implementation has been challenging.”).

in the aggression by which enforcement agencies go after U.S. firms in the market and novel enforcement tactics.<sup>54</sup>

There have been concerning occasions in the past where the Indian government has blocked websites or made requests to take down specific content.<sup>55</sup> However, recent legislative changes relating to digital services will pose greater challenges to U.S. exporters in India's vibrant digital market.<sup>56</sup> Earlier this year, amendments to India's Information Technology Act, 2000 Act went into effect imposing additional requirements under the Intermediary Guideline Rules 2011, imposing new obligations on intermediaries.<sup>57</sup> These include strict timelines for takedown requests, and impose significant penalties for noncompliance. These revisions also include localization requirements, and traceability requirements which pose greater security risks. Specifically, the new rules replaced the 2011 Information Technology (Intermediary Guidelines) Rules and introduced new obligations on online intermediaries. Intermediaries must remove certain content within 24 hours upon receipt of a court order or Government notification, and deploy tools to proactively identify and remove unlawful content. There are also concerning law enforcement assistance provisions, including a requirement for intermediaries to "enable tracing out of such originators of information on its platform" at the request of government officials, as well as local incorporation and local presence requirements. While there was a public consultation on the proposed changes in 2018, there was limited opportunity for industry and other stakeholders to provide input as the draft amendments and new obligations developed.<sup>58</sup>

---

<sup>54</sup> *Twitter Says It's Concerned with India's Intimidation, Requests 3 More Months to Comply With New IT Rules*, TECHCRUNCH (May 27, 2021), <https://techcrunch.com/2021/05/27/twitter-says-concerned-with-india-intimidation-requests-3-more-months-to-comply-with-new-it-rules/>.

<sup>55</sup> See CCIA Comments to USTR for 2019 National Trade Estimate Report, filed Oct. 2018, available at <https://www.ccianet.org/wp-content/uploads/2018/10/CCIA-Comments-to-USTR-for-2019-NTE.pdf> at 58-60.

<sup>56</sup> *India: An Update on India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, Global Advertising Lawyers Alliance (GALA) (June 2, 2021), <https://www.mondaq.com/india/social-media/1074774/an-update-on-india39s-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021>.

<sup>57</sup> The Indian Government Press Release is available at <https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1700749>, and the full text is available at <https://egazette.nic.in/WriteReadData/2021/225464.pdf>.

<sup>58</sup> CCIA had filed comments in the 2018 public consultation regarding proposed amendments to the Information Technology (Intermediary Guidelines) Rules 2011. Available at <https://www.ccianet.org/wp-content/uploads/2019/02/Comments-of-CCIA-to-MeitY-on-Draft-Intermediary-Guidelines-2018-1.pdf>.

Companies make determinations on how they want to operate in response to the new rules, as well as the increased enforcement tactics by Indian officials. Under the new rules, the Indian government is already asserting that at least one U.S. firm should be stripped of liability protection for user content.<sup>59</sup>

### **J. Korea**

Rules announced in 2019 by the Korean Communications Commission will enable officials to filter online content and block websites based outside the country.<sup>60</sup> While in the pursuit of enforcing existing laws regarding illegal content, some have raised concerns that the framework follows authoritarian models of Internet regulation and the extraterritoriality implications.<sup>61</sup>

### **K. Nigeria**

In June 2021, Nigeria announced an “indefinite ban” on Twitter in the country following the company’s decision to remove posts from political leaders that violated its abusive behavior policy. Cases like this illustrate the challenges online businesses face with respect to proactively removing content that violates their terms of service, which are crafted to ensure harmful content is quickly removed. As reported, most telecommunications providers quickly complied, even though the policy was not passed through legislation and could be subject to litigation on the basis of free speech.<sup>62</sup>

### **L. Russia**

Russia continues to serve as a model of government imposed control of Internet services and speech online. As detailed below, in recent years Russia has passed many new laws that grant Russian authorities greater control over online communications and services, as well as impose a number of obligations on services to comply with government demands. The most

---

<sup>59</sup> *Twitter Has Lost Liability Protection in India Government Says*, TECHCRUNCH (July 6, 2021), <https://techcrunch.com/2021/07/06/twitter-has-lost-liability-protection-in-india-government-says/>.

<sup>60</sup> Press Release, Korean Communications Commission, 방통위, 불법정보를 유통하는 해외 인터넷사이트 차단 강화로 피해구제 확대 [“KCC Expands Relief Measures by Strengthening Blocking of Overseas Internet Sites that Distribute Illegal Information”].

<sup>61</sup> NEW AMERICA, *Analysis: South Korea’s New Tool for Filtering Illegal Internet Content* (Mar. 15, 2019), <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/analysis-south-koreas-sni-monitoring/>; *Is South Korea Sliding Toward Digital Dictatorship?*, FORBES (Feb. 25, 2019), <https://www.forbes.com/sites/davidvolodzko/2019/02/25/is-south-korea-sliding-toward-digital-dictatorship/>

<sup>62</sup> *Nigeria’s Twitter Ban is Another Sign Dictatorship is Back*, FOREIGN POLICY (June 7, 2021), <https://foreignpolicy.com/2021/06/07/nigeria-twitter-ban-dictatorship/>.



recent laws include Federal law N482-FZ and Federal law N511-FZ, which came into effect in 2021.<sup>63</sup> Under Federal law N482-FZ, certain platforms can be fined or blocked (through explicit blocking or throttling of Internet traffic) for removing or restricting access to content by the Russian media.<sup>64</sup> Federal law N511-FZ imposes fines for services that do not remove banned information, which has included political protest content.<sup>65</sup> In recent months, U.S. firms have experienced an increase in demands by the *Roskomnadzor*, which regulates Internet services, to take down content, including through requests pursuant to these new rules.<sup>66</sup> Firms that Russian authorities determine have not sufficiently complied with demands have experienced an uptick in throttling and restriction in services.<sup>67</sup>

In May 2019, the Russian government enacted legislation that will extend Russia's authoritarian control of the Internet by taking steps to create a local Internet infrastructure. The law (Federal law N90-FZ) permits Russia to establish an alternative domain name system for Russia, disconnecting itself from the World Wide Web and centralizing control of all Internet traffic within the country.<sup>68</sup>

In March 2019, Russia passed two laws aimed at eliminating "fake news". The Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies and Protection of Information<sup>69</sup> and the Federal Law on Amending the Code of Administrative Violations,<sup>70</sup> establish penalties for "knowingly spreading fake news" and establish a framework for ISPs to block access to websites deemed to be spreading "fake news."

In December 2019, Russia adopted a law that requires the pre-installation of Russian

---

<sup>63</sup> Baurzhan Rakhmetov, *The Putin Regime Will Never Tire of Imposing Internet Control: Development in Digital Legislation in Russia*, COUNCIL ON FOREIGN RELATIONS (Feb. 22, 2021), <https://www.cfr.org/blog/putin-regime-will-never-tire-imposing-internet-control-developments-digital-legislation-russia>.

<sup>64</sup> *Id.*

<sup>65</sup> *Id.*

<sup>66</sup> *Russia Raises Heat on Twitter, Google and Facebook in Online Crackdown*, N.Y. TIMES (May 26, 2021), <https://www.nytimes.com/2021/05/26/technology/russia-twitter-google-facebook-censorship.html>.

<sup>67</sup> *How Russia is Stepping Up Its Campaign to Control the Internet*, TIME (Apr. 1, 2021), <https://time.com/5951834/russia-control-internet/>; *New Russia Bill Would Expand Internet Censorship*, HRW Warns, RADIO FREE EUROPE (Nov. 24, 2020), <https://www.rferl.org/a/hrw-warns-new-russian-bill-would-expand-internet-censorship/30966049.html>.

<sup>68</sup> *Putin Signs 'Russian Internet Law' to Disconnect Russia From the World Wide Web*, FORBES (May 2, 2019), <https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/>

<sup>69</sup> Available at <http://publication.pravo.gov.ru/Document/View/0001201903180031> [Russian].

<sup>70</sup> Available at <http://publication.pravo.gov.ru/Document/View/0001201903180021> [Russian].

software on certain consumer electronic products sold in Russia and sets a dangerous precedent.<sup>71</sup> The law took effect in early 2021.<sup>72</sup> The scope of devices is likely to include smartphones, computers, tablets, and smart TVs, and the scope of applications is likely to include search engines, navigation tools, anti-virus software, software that provides access to e-government infrastructure, instant messaging and social network software, and national payment software.

As noted above, Russia is also a country that imposes restrictions on the use of tools to circumvent censorship methods and access restricted content or services. Pursuant to a 2018 law, search engines are fined for providing access to “proxy services” including VPNs.<sup>73</sup>

### **M. Singapore**

The Protection from Online Falsehoods and Manipulation Bill became effective starting on October 2, 2019.<sup>74</sup> The law requires online services to remove content or carry ‘corrections’ on their platforms in response to claims from the government or from individuals that content is false or misleading.<sup>75</sup> It places too much power to determine falsehoods in the hands of the government without adequate and timely oversight processes, particularly by the judiciary. Instead of enhancing trust online, these rules could spread more misinformation while restricting platforms’ ability to continue to address misinformation issues. There are also threats to undermine security and privacy.<sup>76</sup> Stakeholders have raised concerns with enforcement of these

---

<sup>71</sup> *Russia Passes Law Forcing Manufacturers to Install Russian-made Software*, THE VERGE (Dec. 3, 2019), <https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphoneslaptops>.

<sup>72</sup> *Russia Law Requires Smart Devices to Come Pre-Installed With Domestic Software*, REUTERS (Apr. 1, 2021), <https://www.reuters.com/article/us-russia-technology-software/russian-law-requires-smart-devices-to-come-pre-installed-with-domestic-software-idUSKBN2BO4P2>.

<sup>73</sup> HUMAN RIGHTS WATCH, *Russia: Growing Internet Isolation, Control, Censorship* (June 18, 2020), <https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship>. The Human Rights Watch identified all the following laws from 2017-2020 that “collectively empower the Russian government to exercise extensive control over the internet infrastructure and online activity in Russia” which include: 2016 “Yarovaya amendments” on forced data retention; 2017 law prohibiting VPNs and internet anonymizers from providing access to banned websites and follow-up 2018 amendments to the Code of Administrative Offenses; 2017 law on identification of messaging application users and a follow-up 2018 government decree; 2019 “Sovereign internet” law; and 2019 law on pre-installed Russian applications.

<sup>74</sup> Republic of Singapore, Protection from Online Falsehoods and Manipulation Act 2019, published on June 25, 2019, <https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625>.

<sup>75</sup> Rachael Stelly, *Singapore’s Dangerous Response to Combating Misinformation Online*, DISRUPTIVE COMPETITION PROJECT (Apr. 25, 2019), <https://www.project-disco.org/21st-century-trade/042519-singapores-dangerous-response-combating-misinformation-online/>.

<sup>76</sup> *This ‘Fake News’ Law Threatens Free Speech. But It Doesn’t Stop There*, N.Y. TIMES (May 30, 2019), <https://www.nytimes.com/2019/05/30/opinion/hate-speech-law-singapore.html>.

laws since it went into effect,<sup>77</sup> and recent use cases of the law involve demands to take down political speech and media platforms ahead of the July 2020 general elections.<sup>78</sup>

## N. Thailand

In November 2019, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what is considered “false and misleading” in violation of the Computer Crimes Act.<sup>79</sup> The government has also issued emergency decrees in relation to the global pandemic that further restrict online and press freedom.<sup>80</sup> In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.<sup>81</sup> Under the new law, officials are granted authority to “search and seize data and equipment in cases that are deemed issues of national emergency.”<sup>82</sup> This could “enable internet traffic monitoring and access to private data, including communications, without a court order.”<sup>83</sup>

## O. Turkey

Turkey remains one of the most restrictive markets for Internet services, and continues to utilize censorship tools to limit online speech.<sup>84</sup> Industry has tracked previous laws that preemptively block websites on vague grounds, and specific instances of blocking by Turkish authorities as areas of concern.<sup>85</sup>

---

<sup>77</sup> *Singapore: ‘Fake News’ Law Curtails Speech*, HUMAN RIGHTS WATCH (Jan. 13, 2021) <https://www.hrw.org/news/2021/01/13/singapore-fake-news-law-curtails-speech>.

<sup>78</sup> *Freedom on the Net 2020: Singapore (2020)*, <https://freedomhouse.org/country/singapore/freedom-net/2020>.

<sup>79</sup> *Freedom on the Net 2020: Thailand (2020)*, <https://freedomhouse.org/country/thailand/freedom-net/2020>.

<sup>80</sup> *Id.*

<sup>81</sup> *See Asia Internet Coalition Statement*, Feb. 28, 2019, [https://aicasia.org/wpcontent/uploads/2019/03/AICStatement\\_Thailand-Cybersecurity-Law\\_28-Feb-2019.pdf](https://aicasia.org/wpcontent/uploads/2019/03/AICStatement_Thailand-Cybersecurity-Law_28-Feb-2019.pdf) (“Protecting online security is a top priority, however the Law’s ambiguously defined scope, vague language and lack of safeguards raises serious privacy concerns for both individuals and businesses, especially provisions that allow overreaching authority to search and seize data and electronic equipment without proper legal oversight. This would give the regime sweeping powers to monitor online traffic in the name of an emergency or as a preventive measure, potentially compromising private and corporate data.”).

<sup>82</sup> *Thailand Passes Controversial Cybersecurity Law*, TECHCRUNCH (Feb. 28, 2019), <https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/>.

<sup>83</sup> *Id.*

<sup>84</sup> *Freedom on the Net 2020: Turkey (2020)*, <https://freedomhouse.org/country/turkey/freedom-net/2020>.

<sup>85</sup> *CCIA Comments to USTR for 2019 NTE*, *supra* note 55 at 74-76. *See also, e.g.*, Alexandra de Cramer, *Silence Descends on Social Media in Turkey*, ASIA TIMES (Sept. 11, 2020), <https://asiatimes.com/2020/09/silence-descends-on-social-media-in-turkey/> (“Ifade Ozgurlugu Platformu, a Turkish Internet-freedom watchdog, reports that at the end of 2019, Turks were denied access to more than 408,000 websites. Twitter’s “transparency report” for the first half of 2019 ranked Turkey in second place globally for taking legal action to remove content.”); *Turkey, Enemy of the Internet?*, REPORTERS WITHOUT BORDERS (Aug. 28, 2014), <http://en.rsf.org/turquie-turkey-enemy-of->

In recent years, the market conditions have worsened. Turkish lawmakers passed legislation (“Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications”<sup>86</sup>) in July 2020 that grants the government sweeping new powers to regulate content on social media.<sup>87</sup> The law went into effect October 1, 2020, and authorities were quick to take action against U.S. firms, imposing fines,<sup>88</sup> advertising bans, and bandwidth restrictions within months.<sup>89</sup> The law requires social network providers with more than one million daily users to: establish a representative office in Turkey, respond to individual complaints in 48 hours or comply with official takedown requests of the courts in 24 hours, report on statistics and categorical information regarding the requests every six months, and take necessary measures to ensure the data of Turkish resident users is kept in country. Social network providers face serious monetary fines and significant bandwidth reduction to their platform in cases of noncompliance.

#### **P. Vietnam**

The Law on Cybersecurity took effect in January 2018 and includes concerning provisions on content regulation, requiring online services to monitor user-generated content and remove “prohibited” content within 24 hours upon notification from government offices. It also establishes procedures for the service provider to both terminate access for a user posting “prohibited” content and share information regarding the user. “Prohibited” content includes content that is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision.<sup>90</sup>

---

the-internet-28-08-2014,46856.html; *Google, Others Blast Turkey Over Internet Clampdown*, WALL ST. J. (Apr. 1, 2014), <https://online.wsj.com/articles/SB10001424052702303978304579473190997035788>; *Major Internet Access Issues in Turkey as Cloudflare Knocked Offline*, TURKEY BLOCKS (June 5, 2017), <https://turkeyblocks.org/2017/06/05/major-internet-access-issues-turkey-cloudflare-knocked-offline>; Emile Aben, *Internet Access Disruption in Turkey 2016* (July 19, 2016), <https://labs.ripe.net/Members/emileaben/internet-access-disruption-in-turkey>.

<sup>86</sup> Available at <https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm>.

<sup>87</sup> *Turkey Passes Law Extending Sweeping Powers Over Social Media*, N.Y. TIMES (July 29, 2020), <https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html>.

<sup>88</sup> *Turkey Fines Social Media Giants for Breaching Online Law*, AP NEWS (Nov. 4, 2020), <https://apnews.com/article/business-turkey-media-social-media-560de2b21d54857c4c6545c1bd20fc25>.

<sup>89</sup> *Turkey Slaps Ad Ban in Twitter Under New Social Media Law*, REUTERS (Jan. 19, 2021), <https://www.reuters.com/article/us-turkey-twitter/turkey-slaps-ad-ban-on-twitter-under-new-social-media-law-idUSKBN29O0CT>.

<sup>90</sup> *Vietnam Says Facebook Violated Controversial Cybersecurity Law*, REUTERS (Jan. 8, 2019), <https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecurity-law-idUSKCN1P30AJ>; *Vietnam Quick to Enforce New Cybersecurity Law*, Hogan Lovells Chronicle of Data

Besides regulatory roadblocks, U.S. companies face challenges from technical intervention such as throttling or limiting server access. These technical interventions are part of the government's effort to influence and control content, and undermine U.S. company competitiveness in the marketplace. At the end of 2020, Vietnamese authorities threatened to shut down Facebook in the country if the U.S. firm did not censor certain political content on its platform at the request of the government.<sup>91</sup>

## V. CONCLUSION

The USITC Investigations present a key opportunity to provide policymakers and other stakeholders an overview of an increasingly concerning trend to digital trade and the future of the open Internet.

July 21, 2021

---

Protection (Mar. 6, 2019), <https://www.engage.hoganlovells.com/knowledgeservices/news/vietnam-quick-to-enforce-new-cybersecurity-law/>.

<sup>91</sup> *Vietnam Threatens to Shut Down Facebook Over Censorship Requests*, REUTERS (Nov. 19, 2020), <https://www.reuters.com/article/vietnam-facebook-shutdown/exclusive-vietnam-threatens-to-shut-down-facebook-over-censorship-requests-source-idUSKBN28007K>.