Before the
Office of the United States Trade Representative
Washington, DC

In re	Docket No. 2015-0014
Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers	

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the request for comments issued by the Office of the United States Trade Representative (USTR) and published in the Federal Register at 80 Fed. Reg. 50,377 (Aug. 19, 2015), the Computer & Communications Industry Association (CCIA) submits the following comments for consideration as the USTR composes its annual National Trade Estimate Report on Foreign Trade Barriers (NTE).

I. INTRODUCTION

CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. CCIA members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[1]

As the Internet evolves into a central component of cross-border trade in both goods and services, the removal of barriers to Internet-enabled international commerce becomes critical to U.S. economic interests. Given U.S. leadership in high-tech innovation and Internet technology, clearing hurdles to the export of Internet-enabled products and services promises huge economic gains. As the U.S. International Trade Commission (ITC) noted in a 2013 report, "[s]tudies that have quantified the economic contributions of the Internet have generally found that it has made significant contributions to U.S. output, employment, consumer welfare, trade, innovation, productivity, and corporate financial performance."[2]

[1] A list of CCIA members is available at https://www.ccianet.org/members.
[2] United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013), http://www.usitc.gov/publications/332/pub4415.pdf.

As CCIA has observed in previous submissions, international markets are increasingly important growth opportunities for U.S. services, even as international competition has grown. In 2014, nine out of the top ten "global Internet properties" were made in the U.S., but 79% of their users came from outside the United States.[3] The United Nations predicts that 300 million more people worldwide will gain regular access to the Internet in 2015, leading in total to 3.2 billion global Internet users.[4]

Despite the increasing importance of Internet-enabled trade, U.S. trade policies and priorities have not sufficiently adapted to reflect that importance to the U.S. economy. While trade policy has dramatically reduced barriers to trade in goods especially, the United States is increasingly becoming a services economy, with service industries employing a large majority of U.S. private-sector workers.[5] Meanwhile, the United States is the largest global exporter of services, exporting $662 billion in 2013 (a growth of 5 percent over the previous year.)[6] The Internet has been the single biggest component of the cross-border trade in services, with many of those services facilitating the international goods trade as well.

As a result of these changes in the structure of the global economy, the U.S. economy has evolved beyond the sectors covered under the robust umbrella of liberalization that has occurred in the international trade system in the last 60 years. To protect U.S. economic interests, U.S. trade policy must prioritize addressing barriers to the Internet and Internet-enabled services, given their key role in the U.S. economy and U.S. export growth.

Adapting to these trends requires increasing the NTE's focus on barriers to digital trade. To that end, these comments identify key obstacles to digital trade, including infrastructure

---

[3] Mary Meeker, *Internet Trends 2014*, May 28, 2014, at 130, http://www.kpcb.com/blog/2014-internet-trends. By way of specific example, Google's total international revenue was 39% of its overall sales in 2005, whereas today 56% of its revenue comes from overseas. *Compare* Press Release, Google, *Google Announces Fourth Quarter and Fiscal Year 2005 Results*, Jan. 31, 2006, https://investor.google.com/earnings/2005/Q4_google_earnings.html *with* Press Release, Google, *Google Announces Fourth Quarter and Fiscal Year 2014 Results*, Jan. 29, 2015, https://investor.google.com/earnings/2014/Q4_google_earnings.html. Similarly, 83% of Facebook's users lie outside of the U.S. and Canada, while fewer than 50% of Facebook users were international as of 2008. *Compare* Facebook Company Info, http://newsroom.fb.com/company-info/ *with* Miguel Helft, *Facebook Makes Headway Around the World*, N.Y. Times, July 7, 2010, http://www.nytimes.com/2010/07/08/technology/companies/08facebook.html.

[4] Tom Miles, *Internet Growth Slows; most people still offline: U.N.*, Reuters, Sept. 21, 2015, http://www.reuters.com/article/2015/09/21/us-internet-un-idUSKCN0RL0VZ20150921

[5] Bureau of Labor Statistics, *Current Employment Statistics, Employees on nonfarm payrolls by industry sector and selected industry detail seasonally adjusted*, http://www.bls.gov/web/empsit/ceseeb1a.htm (last modified Oct. 2, 2015).

[6] World Trade Organization, *International Trade Statistics 2014* (2014), at 17, 28, https://www.wto.org/english/res_e/statis_e/its2014_e/its2014_e.pdf.

localization mandates, the filtering and blocking of Internet content, poorly tailored intellectual property laws, and onerous intermediary liability regimes. Traditional trade and non-tariff barriers, such as onerous customs procedures and duties for small shipments, postal policies, housing rental and taxi regulations, and outdated financial services regulations should also receive continued attention from USTR.

II. DATA AND INFRASTRUCTURE LOCALIZATION

As CCIA has noted in previous filings, countries continue to show interest in implementing data localization policies, which include mandated server localization and data storage. Accelerated by the impact of the Snowden revelations, the number of countries imposing or considering data and infrastructure localization requirements has increased in recent years. Stated motivations for these policies include the desire to ensure domestic privacy protections, to protect against foreign espionage, to guarantee law enforcement access to personal data, and to promote local economic development.

Political motivations aside, data localization requirements in fact tend to undermine their stated goals. Rather than ensuring user privacy or data security, forced localization creates a host of new targets of opportunity for hackers, criminals and foreign intelligence agencies.[7] Data localization rules often centralize information in hotbeds for digital criminal activity, including Indonesia, Brazil, Vietnam, and Russia, working against data security best practices that emphasize decentralization over single points of failure.[8]

Even as tools of protectionism, which the global trade system was built to oppose, data localization policies are likely to hinder economic development, rather than promote domestic industry.[9] As the McKinsey Global Institute documented in 2011, 75% of the value of the Internet accrues to traditional, non-Internet centric businesses through productivity gains and

[7] Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, UC Davis Legal Studies Research Paper No. 378, Apr. 2014, at 32, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858 (hereinafter "Chander & Le").

[8] Rohin Dharmakumar, *India's Internet Privacy Woes*, Forbes India, Aug. 23, 2013, http://forbesindia.com/article/checkin/indias-internet-privacy-woes/35971/1. *See generally* Patrick S. Ryan *et al*., *When the Cloud Goes Local: The Global Problem with Data Localization*, IEEE Computer, vol. 46, no. 12, pp. 54-59 (Dec. 2013) http://www.computer.org/csdl/mags/co/2013/12/mco2013120054-abs.html.

[9] Leviathan Security Grp., *Quantifying the Costs of Forced Localization* (2015), http://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

easier access to foreign markets.[10] As a result, such policies will invariably harm a wide swath of traditional domestic economic activity and harm a country's global competitiveness.[11] Not surprisingly, economists at the European Centre for International Political Economy (ECIPE) found that current data localization proposals will have significant negative domestic economic effects on the countries adopting or contemplating them.[12]

To remain compliant with international trade rules, measures that restrict trade in services must be necessary to achieve specific legitimate national security or public policy objectives, and must not be applied in a discriminatory manner or in a way that amounts to a disguised restriction on trade in services. As discussed below, data localization mandates almost invariably fail to meet this standard. In addition, these regulations are often vaguely construed, inadequately articulated and, therefore, nearly impossible to effectively implement.[13] What follows is a non-exhaustive list highlighting a few examples of potentially trade-restrictive localization policies or policy proposals:

Russia

As CCIA observed in its 2014 NTE submission, Russia signed localization measures into law in July of 2014,[14] which went into effect on September 1, 2015. The law requires all operators that process the personal data of Russian citizens to use databases located exclusively in Russia, and to disclose the address of these databases to the Russian telecommunications authority. In August 2015, the Ministry of Communications and Mass Media issued 'clarifications' explaining the law's provisions, indicating that the localization requirements will

[10] Matthieu Pélissié du Rausas *et al*., McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity* (2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

[11] For example, foreign investment will likely decline. Given the high cost of constructing data centers, many companies will simply opt out of serving markets with onerous data localization requirements, especially small- and medium-sized businesses. In 2013, the average cost of data centers in Brazil and Chile were $60.3 million and $43 million, respectively. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, Wall St. J., Nov. 13, 2013, http://online.wsj.com/articles/SB10001424052702304868404579194290325348688.

[12] Matthias Bauer *et al*., *The Costs of Data Localization: Friendly Fire on Economic Recovery*, ECIPE (2014), http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.

[13] *See* Chander & Le; United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2* (2014), http://www.usitc.gov/publications/332/pub4485.pdf (hereinafter "*Digital Trade in the U.S. and Global Economies, Part 2*").

[14] Paul Sonne, *Russia Steps Up New Law to Control Foreign Internet Companies*, Wall St. J., Sept. 24, 2014, http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

apply to business activities which are "oriented towards" a Russian audience.[15] Despite these clarifications, experts are concerned about the broad language of the rule which would indicate that all multinational companies with Russian customers must comply,[16] as well as the requirements to inform Russia's telecommunications authorities.[17]

ECIPE predicts that, due to productivity losses associated with these policies, the Russian economy would shrink by 286 billion rubles (equivalent to $5.7 billion or -0.27% of GDP). Further, investment would drop by -1.41% or 187 billion rubles.[18] These losses also reflect lost export opportunities for U.S. service providers.

India[19]

Through amendments in 2011 to its Information Technology Act of 2000, India has restricted the transfer of data in cases only "if it is necessary for the performance of the lawful contract" or when the data subject consents to the transfer. However, the necessity requirement is not adequately explained, effectively limiting transfer of data only when consent is given. India has also taken steps to avoid U.S.-based service providers in internal government communications, relying on interpretations of their Public Records Act of 1993. Proposed policies seek to mandate that all employees only use government email services and that agencies host their websites on servers within India, and to restrict use of private services regardless of geographic origin. As CCIA noted in its prior submission, Indian authorities have contemplated extending localization policies to non-government communications as well,[20]

[15] Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, Bloomberg BNA, Aug. 10, 2015, http://www.bna.com/russia-clarifies-looming-n17179934521/.

[16] News outlets have reported that the telecommunications authority has a list of 317 companies it will seek to investigate by the end of the year, and which may be banned from doing business in Russia if they are not found in compliance with the law. This may set a precedent for denial of market access in violation of Russia's trade agreements. *See, e.g.*, Georgy Bovt, *Will Data Law Isolate Russia Further? (Op-Ed)*, Moscow Times, Sept. 1, 2015, http://www.themoscowtimes.com/opinion/article/will-data-law-isolate-russia-further-op-ed/529229.html

[17] Courtney M. Bowman, *Primer on Russia's New Data Localization Law*, Nat'l Law Review, Aug. 28, 2015, http://www.natlawreview.com/article/primer-russia-s-new-data-localization-law/.

[18] Matthias Bauer, Hosuk Lee-Makiyama, & Erik van der Marel, *Data Localisation in Russia: A Self-imposed Sanction* (European Centre for International Political Economy June 2015), http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/.

[19] Chander & Le at 16-19; *Avoiding NSA clutches: India to launch internal email policy for government communications*, RT, Oct. 31, 2013, http://rt.com/news/india-nsa-internal-email-994/.

[20] Thomas K. Thomas, *National Security Council proposes 3-pronged plan to protect Internet users*, The Hindu Business Line, Feb. 13, 2014, http://www.thehindubusinessline.com/info-tech/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

which would require all private data of Indian citizens be stored on servers within the country and prevent the mirroring of data on servers abroad.[21]

China

Chinese authorities have issued comprehensive guidelines for the treatment of personal data within information systems, requiring either (1) express consent of data subject or (2) explicit regulatory or legal approval before personal data may be transferred abroad. National security regulations also prevent the transfer of data abroad if it contains a state secret, which includes all communication of "matters that have a vital bearing on state security and national interests." The Chinese government also practices strong protectionism in their information technology industries. Foreign companies operating in cloud computing are forced to enter into joint partnerships with Chinese firms if they wish to conduct business within China[22] and industry representatives have cited their inability to obtain Internet service provider licenses in China without partnering with a domestic company that holds a license. China, along with Taiwan, Turkey, and India, also implements local-presence requirements for processing of payment transactions.[23]

A recent report by the American Chamber of Commerce in China surveyed existing and proposed Chinese data localization policies and found the following:[24]

1. *The Law of the People's Republic of China on Guarding State Secrets* [National People's Congress (NPC), 1989, revised 2010]: Prevents data from being removed from China if it is deemed to contain a state secret. State secrets include "matters that have a vital bearing on state security and national interests."

2. *Notice to Urge Banking Financial Institutions to Protect Personal Information* [People's Bank of China (PBOC), 2011]: Law that prohibits financial institutions from analyzing, processing, or storing offshore personal financial information of Chinese citizens.

3. *Information Security Technology – Guidelines for Personal Information Protection*

[21] Like many other countries, India may be contemplating data localization as an economic investment strategy: ECIPE estimates predict that India's data localization efforts will lead to a 1.4% decrease in domestic investment. *See* Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 3/2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[22] U.S.-China Economic and Security Review Commission, *Red Cloud Rising: Cloud Computing in China*, Sept. 2013, revised Mar. 2014, at 5, http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf.

[23] *Digital Trade in the U.S. and Global Economies, Part 2* at 86.

[24] AmCham China, *Protecting Data Flows in the US-China Bilateral Investment Treaty*, Apr. 2015, at 4, http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization.

within Public and Commercial Services Information Systems [Standardization Administration of China & General Administration of Quality Supervision, Inspection and Quarantine, 2013]: Standard that prohibits the overseas transfer of data to an entity without express user consent or government permission.

4. *Administrative Regulation on Credit Information Industry* [State Council, 2013] & *Administrative Measures for Credit Reference Agencies* [PBOC, 2013]: State Council Law and PBOC standard which require that any credit information collected within the territory of China be organized, stored and processed within China. Credit reporting agencies must have back up databases established in China and may not transmit any information collected thereby outside of China through the Internet or storage media.

5. *Counter-terrorism Law* [NPC, 2014]: Draft law that requires Internet and telecommunication companies to store data on Chinese servers, create methods for monitoring content for terror threats, and provide encryption keys to public security authorities. In an interview with Reuters, President Obama said that the law's provisions "would essentially force all foreign companies, including U.S. companies, to turn over to the Chinese government mechanisms where they can snoop and keep track of all the users of those services."[25]

6. *Guiding Opinions for Promoting the Innovation and Development of Cloud Computing to Cultivate New Types of Information Industry Services* [State Council, 2014]: Guidelines that serve as framework for future cloud computing laws and regulations. References the importance of regulating cross-border data flows.

7. *Population Health Information Management (Pilot)* [National Health and Family Planning Commission, 2014]: Prohibits the storage of individual personal health information in overseas data centers.

A draft of a new cybersecurity law, which was released for comment by China in July, is also a cause for concern. In its current version, the law would require security reviews on procurement in a wide variety of fields as well as on data exported out of China.[26] The law also requires that, "information collected or generated by key information infrastructure facilities that is deemed 'important' or 'critical' by the Chinese Government be stored exclusively within

[25] Jeff Mason, *Exclusive: Obama sharply criticizes China's plans for new technology rules*, Reuters, Mar. 3, 2015, http://www.reuters.com/article/2015/03/03/us-usa-obama-china-idUSKBN0LY2H520150303

[26] Gillian Wong, *China to Get Tough on Cybersecurity*, Wall St. J., July 9, 2015, http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416.

mainland China."[27] This law, while still in draft form, reflects an effort by the Chinese government to centralize cybersecurity policy at a national level, rather than in lower-level regulations or private contracts.[28]

While China recently suspended rules which would have forced banks to turn over proprietary source code and encryption keys to the China Banking Regulatory Commission,[29] there are reports that the CBRC has reached out to western technology companies to get opinions on a new version of the rules.[30]

France

France has made significant investments in Numergy and Cloudwatt, local cloud computing firms, to establish a local infrastructure for data storage and processing, known as "*le cloud souverain.*"[31] Furthermore, the French government's cybersecurity agency has proposed guidelines for cloud computing that include forced data localization.[32]

Proposals have also been made to impose a tax on the usage of personal data created in France if the usage is not within the confines of French privacy requirements.[33]

Germany

France's efforts regarding localization have been mirrored in Germany along with calls for a European data network.[34] Deutsche Telekom, the partially state-owned, largest telecommunications provider in Germany, has proposed a "Schengen area routing", which would limit data transfers to between European countries that have removed passport controls. Also, several German email companies have recently launched a service entitled "E-Mail made in

[27] Cheng Lim & Jack Maher, *China lays down the cyber law: Play in our space, play by our rules*, The Interpreter, Oct. 14, 2015, http://www.lowyinterpreter.org/post/2015/10/14/Chinas-lays-down-the-cyber-law-Play-in-our-space-play-by-our-rules.aspx (hereinafter "Lim & Maher").

[28] Austin Ramzy, *What You Need to Know About China's Draft Cybersecurity Law*, N.Y. Times, July 9, 2015, http://sinosphere.blogs.nytimes.com/2015/07/09/what-you-need-to-know-about-chinas-draft-cybersecurity-law/.

[29] Gillian Wong, *China Halts Implementation of Banking-Technology Rules*, Wall St. J., Apr. 16, 2015, http://www.wsj.com/articles/china-halts-implementation-of-banking-tech-guidelines-1429181094.

[30] Lim & Maher.

[31] Chander & Le at 11-12.

[32] *Appel public à commentaires sur le référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage*, Aug. 11, 2014, http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestataires-de-services-securises-dinformatique-en-nuage/.

[33] Chander & Le at 12-13.

[34] Alison Smale, *Merkel Backs Plan to Keep European Data in Europe*, Int'l N.Y. Times, Feb. 16, 2014, http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html.

Germany", which claims to route data only through domestic servers.[35] Although the idea of "Schengen area routing" has fallen out of favor as of late, USTR should be watchful of similar ideas in the future.

In May 2015, Germany adopted a draft telecom bill that would, among other things, require telecoms and Internet service providers to store data in Germany for a period of 10 weeks.[36] Under the draft law, data needing to be stored includes phone numbers, times called, IP addresses, and the international identifiers of mobile users for both ends of a call. Furthermore, user location data in the context of mobile phone services would have to be retained[37] for a period of four weeks.[38] The German Bundestag approved the bill in October 2015.[39]

German policymakers have recently considered policies aimed at a federal government cloud. Referred to as Resolution 2015/5, these policies are ostensibly aimed at streamlining government IT systems and service centers. They also require that "sensitive" information must be localized on servers inside Germany, and further mandate that cloud suppliers guarantee that information not be subject to any disclosure obligations in foreign jurisdictions. While policymakers might reasonably impose certain security-related limits to some sets of secure data, centralization and streamlining efforts may effectively result in the application of localization mandates to all government services. Like other data localization measures discussed in this section, this may discriminate against foreign suppliers and be a violation of WTO commitments.

---

[35] Michael Birnbaum, *Germany looks at keeping its Internet mail traffic inside its borders*, Wash. Post, Nov. 1, 2013, http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html.

[36] Glyn Moody, *Germany's data retention bill requires metadata to be kept in the country*, Ars Technica UK, May 19, 2015, http://arstechnica.co.uk/tech-policy/2015/05/germanys-data-retention-bill-requires-metadata-to-be-kept-in-the-country/.

[37] Many companies have already been moving data resources to Germany preemptively out of general political pressure. *See* Katharine Kendrick, *Risky Business: Data Localization*, Forbes, Feb 19, 2015, http://www.forbes.com/sites/realspin/2015/02/19/risky-business-data-localization/.

[38] Hunton & Williams Privacy & Information Security Law Blog, *Germany Adopts a Draft Telecom Data Retention Law that Includes a Localization Requirement*, June 4, 2015, https://www.huntonprivacyblog.com/2015/06/04/germany-adopts-telecom-data-retention-law-includes-localization-requirement/.

[39] Deutsche Welle, *German parliament votes for new data retention law*, Oct. 16, 2015, http://www.dw.com/en/german-parliament-votes-for-new-data-retention-law/a-18786345. Such bills have not come without controversy in Germany, do to the automatic nature of the data retention. The German Federal Constitutional Court struck down a previous data retention bill in 2010, citing concerns about data security. *See* Dr. Jan Geert Ments et al., *Germany: new data retention act – retention obligations for telecommunications and internet access service providers*, Lexology, Oct. 16, 2015, http://www.lexology.com/library/detail.aspx?g=a17dcbf9-dec8-40f5-9950-04bee4a4894a.

The requirements that service providers ensure that foreign jurisdictions cannot obtain the data would also impose German law unilaterally on international operators wherever they are based.[40]

Nigeria

In December 2013, the National Information Technology Development Agency (NITDA), an agency of the Federal Ministry of Communication Technology, issued the Guidelines for Nigerian Content Development in the ICT sector. The guidelines require that within three years, makers of original ICT equipment utilize at least 50 percent of local manufactures in their products, and that ICT companies generally must use Nigerian companies to provide 80 percent of "value added services" on their networks. Other sections of concern require that all government data be hosted locally (unless officially exempted) and that all subscriber and consumer data be locally hosted. As of May 2015, no clarification has been given regarding the sanctions U.S. companies may face for not complying with the guidelines.

As a State Department report earlier this year described the guidelines, "The goal is to promote development of domestic production of ICT products and services for the Nigerian and global markets, but the guidelines post impediments and risks to foreign investment and U.S. companies by interrupting their global supply chain, increasing costs, disrupting global flow of data, and stifling innovative products and services."[41] An industry report claims the guidelines "will prop up domestic technology enterprises at the expense of higher quality and/or more efficient foreign ones."[42]

Indonesia

Since 2012, service providers providing a "public service" have been required to have data servers within the country. The Ministry of Communication has also recently sought to require domestic data centers for purposes of disaster recovery, extending the mandate to all information technology providers.[43]

---

[40] Hosuk Lee-Makiyama & Matthias Bauer, *The Bundes Cloud: Germany on the Edge to Discriminate Against Foreign Suppliers of Digital Services*, ECIPE, Sept. 2015, http://ecipe.org/publications/the-bundes-cloud-germany-on-the-edge-to-discriminate-against-foreign-suppliers-of-digital-services/?chapter=all.

[41] U.S. Department of State, *Nigeria Investment Climate 2015*, May 2015, at 13, http://www.state.gov/documents/organization/241898.pdf

[42] Michelle A. Wein, *The Worst Innovation Mercantilist Policies of 2014*, ITIF, Dec. 2014, http://www2.itif.org/2014-worst-mercantilist-fourteen.pdf

[43] Chander & Le at 19-20.

Vietnam

The Decree on Management, Provision, and Use of Internet Service and Information Content Online imposes a mandate on Internet service providers to maintain a copy of all data they hold within Vietnam for purposes of access by the Vietnamese authorities.[44] This law has been accompanied by numerous burdensome regulations service providers must adhere to, including local storage of user registration information and complete histories of posting activities on "general information websites" and social networks. These "general information websites" and social networks must also have a high-level representative of the company be a Vietnamese national and local resident.[45]

The Vietnamese authorities are also considering other forms of forced localization. For instance, the draft decree on IT services would require offshore web-based services to establish a local representative in the country in order to continue providing the service to Vietnamese companies and individuals. Insofar as the Trans-Pacific Partnership may contain binding obligations regarding cross-border provision of services as well as transfers of information,[46] policies such as this should be considered if and when Vietnam were to implement that agreement.

III. FILTERING AND BLOCKING

Perhaps the most apparent barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content. Governments continue to filter and block Internet content, platforms and services for various reasons. In its 2014 report, Freedom House assessed that global Internet freedom had declined for the fourth consecutive year due to growing online censorship and monitoring practices.[47] It also reported that between May 2013 and May 2014, 41 countries passed or proposed legislation to "penalize legitimate forms of speech online, increase government powers to control content, or expand government surveillance

[44] *Id.* at 23.
[45] *Id.* at 24.
[46] Office of the United States Trade Representative, *The Trans-Pacific Partnership: Promoting Digital Trade*, https://ustr.gov/tpp/#promoting-digital-trade.
[47] Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, & Mai Truong, *Freedom on the Net 2014: Tightening the Net: Governments Expand Online Controls*, Freedom House, 2014, https://freedomhouse.org/sites/default/files/resources/FOTN%202014%20Summary%20of%20Findings.pdf (hereinafter "Freedom House 2014").

capabilities."[48] Whether deliberate 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; it also immediately affects content providers, advertisers, and small businesses using the service to find and interact with new and existing customers. Such blocking is likely to violate World Trade Organization rules on market access and national treatment, among other international commitments.

Censorship methods vary, but generally consist of legal or regulatory obligations imposed upon intermediary services, network-level blocking and/or filtering achieved through state control of or influence over communications infrastructure, or technology mandates that either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology. Known offenders who use some or all of these practices include Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran, Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.

States are often disinclined to explain or justify blocking Internet content, and in many cases restrictions are not developed in a transparent manner. This lack of clarity is sometimes used against foreign firms, to the advantage of domestic ones.[49] 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 (QoS) of foreign websites and services vis-à-vis domestic Internet content.[50]

Currently, the most problematic trade-related blocking and filtering practices are associated with the following nations:

China

As CCIA explained to the U.S.-China Economic and Security Review Commission earlier this year, barriers to digital trade in China continue to present significant challenges to

[48] *Id.* at 4.
[49] *Digital Trade in the U.S. and Global Economies, Part 2* at 98.
[50] *See* Paul Mozur & Carlos Tejada, *China's 'Wall' Hits Business*, Wall St. J., Feb. 13, 2013, http://online.wsj.com/articles/SB10001424127887323926104578277511385052752.

U.S. exporters.[51] High-profile examples of targeted blocking of whole services include China's blocking of major U.S. services including Facebook, Picasa, Twitter, Tumblr, Google search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare.[52] Informal estimates suggest that this blocking has easily cost American firms billions of dollars as they are pushed out of the market.[53] AmCham China's 2015 Business Climate Survey also found that 83% of U.S. companies doing business in China see Internet restrictions as either "somewhat negatively" or "negatively" impacting their capacity to do business there,[54] while the 2013 survey noted that 62% said search engine disruption made it more difficult to obtain market data, share information, or collaborate with colleagues.[55] A EuroCham survey showed that 13% of respondents had recently deferred R&D investment in China or had become unwilling to set up R&D operations after Internet restrictions increased in early 2015.[56] Numerous scholars have argued that China's actions could violate WTO rules mandating open access and equitable treatment between foreign and domestic firms.[57]

The July draft cybersecurity law mentioned in the previous section also has a provision that would authorize Chinese authorities to terminate Internet access during "public security" emergencies.[58]

China has recently taken several steps to crack down on Internet tools to get around its broad Internet firewall. In January, China made moves to upgrade its Internet firewall by making it harder for people to use VPNs to circumvent it,[59] and recently the country started

[51] *See* Matthew Schruers, Testimony before the U.S.-China Economic and Security Review Commission, *Commercial Espionage and Barriers to Digital Trade in China*, June 15, 2015 *at* http://www.uscc.gov/sites/default/files/Schruers%20Testimony.pdf.

[52] *Digital Trade in the U.S. and Global Economies, Part 2* at 98.

[53] Julie Makinen, *Chinese censorship costing U.S. tech firms billions in revenue*, Los Angeles Times, Sep. 22, 2015, http://www.latimes.com/business/la-fi-china-tech-20150922-story.html

[54] AmCham China, *China Business Climate Survey Report*, 2015, at 30, http://www.amchamchina.org/policy-advocacy/business-climate-survey/.

[55] Christina Larson, *Chinese Censors Slow the Net – and U.S. Businesses*, Businessweek, Apr. 1, 2013, http://www.businessweek.com/articles/2013-04-01/chinese-censors-slow-the-net-and-with-it-u-dot-s-dot-businesses.

[56] EU Chamber of Commerce in China, *Internet Restrictions Increasingly Harmful to Businesses, Say European Companies in China*, Feb. 12, 2015, http://www.europeanchamber.com.cn/en/press-releases/2235

[57] Kevin Holden, *Breaking Through China's Great Firewall*, The Diplomat, July 30, 2014, http://thediplomat.com/2014/07/breaking-through-chinas-great-firewall/

[58] Wong, *China to Get Tough on Cybersecurity*, *supra* note 26.

[59] Elizabeth Weise & Calum MacLeod, *China Blocks VPN Access to the Internet*, USA Today, Jan. 24, 2015, http://www.usatoday.com/story/tech/2015/01/23/china-internet-vpn-google-facebook-twitter/22235707/.

cracking down on special software tools hosted on GitHub, a website popular with open source enthusiasts.[60]

Turkey

CCIA has previously noted barriers to social media such as Twitter and YouTube in Turkey,[61] which adopted laws in February 2014 "allowing it to 'preventively' block websites on such vague grounds as the presence of content that is 'discriminatory or insulting towards certain members of society.'"[62] The recent unrest in Syria has led to further government censorship, with Turkish authorities recently censoring websites and Twitter accounts accused of spreading Kurdish propaganda, including journalism sites.[63]

Pakistan

As CCIA has previously noted, YouTube has been blocked in Pakistan since September 2012. While several legislative committees in Pakistan have recently urged for legislation unblocking YouTube, the nation's IT Ministry informed legislators that only a court decision could overrule the ban, leaving industry to attempt to negotiate workarounds.[64] In 2013, Pakistan's new minister for IT and telecommunications had threatened to block the Google search engine as well, and declared that YouTube would remain blocked until it employed a filter to "screen out blasphemous and pornographic content."[65] The popular blog site WordPress was also temporarily blocked for several days earlier this year with little explanation from authorities.[66]

Both Twitter and Facebook have intermittently been blocked in Pakistan, while Facebook

[60] Michael Kan, *China intensifies Internet censorship ahead of military parade*, PC World, Aug. 30, 2015, http://www.pcworld.com/article/2977109/china-intensifies-internet-censorship-ahead-of-military-parade.html.

[61] Joe Parkinson *et al*., *Turkey's Erdogan: One of the World's Most Determined Internet Censors*, Wall St. J., May 2, 2014, http://online.wsj.com/articles/SB10001424052702304626304579505912518706936.

[62] Reporters Without Borders, *Turkey, Enemy of the Internet?*, Aug. 28, 2014, http://en.rsf.org/turquie-turkey-enemy-of-the-internet-28-08-2014,46856.html; Emre Peker, Joe Parkinson & Sam Schechner, *Google, Others Blast Turkey Over Internet Clampdown*, Wall St. J., Apr. 1, 2014, http://online.wsj.com/articles/SB10001424052702303978304579473190997035788.

[63] Zeynep Karataş, *Ongoing censorship blocks Kurdish, critical, data-based media during time of crisis*, Today's Zaman, Aug. 15, 2015, http://www.todayszaman.com/anasayfa_ongoing-censorship-blocks-kurdish-critical-data-based-media-during-time-of-crisis_396569.html.

[64] *Senate body seeks legislation to lift YouTube ban*, Dawn, Sept. 15, 2015, http://www.dawn.com/news/1207132.

[65] Rob Crilly, *Pakistan threatens to ban Google unless it cleans up YouTube*, The Telegraph, June 11, 2013, http://www.telegraph.co.uk/news/worldnews/asia/pakistan/10112655/Pakistan-threatens-to-ban-Google-unless-it-cleans-up-YouTube.html.

[66] Bina Shah, *WordPress Ban,* Dawn, Mar. 26, 2015, http://www.dawn.com/news/1171842.

is also routinely asked by the government to censor material deemed 'blasphemous'.[67]

Iran

In May 2014, Iran blocked access to Google's hosting platform, Google Sites, and censored at least two Wikipedia pages.[68] The country also continues to block Twitter and Facebook, while some government officials have pushed to block WhatsApp and Viber.[69] Freedom House also ranked Iran as the worst country for Internet freedom in its 2014 report.[70] In late 2014, reports from Iran suggested that the country would impose a filtering system, rather than blocking websites outright. The approach would still be used to filter content which is 'criminal' for moral or political reasons.[71]

Russia

Russia's 2012 Internet blacklist law, depending how expansively it is used, has the potential to block numerous American owned websites and services.[72] According to Freedom House, "blocking access to information on entire websites, IP addresses, and particular webpages has become the most common means in Russia to restrict user activity on the Internet."[73]

In August 2015, Russia temporarily took down the entire Wikipedia site, reportedly in response to a page regarding the preparation of a form of cannabis called charas. After the page was edited to meet authorities' approval, the site came online again.[74] Russia also temporarily suspended Reddit in summer 2015 after a Russian user posted about psychedelic mushrooms.

---

[67] *See* Gibran Ashraf, *Facebook censored 54 posts for 'blasphemy' in Pakistan in second half of 2014*, The Express Tribune, Mar. 18, 2015, http://tribune.com.pk/story/855030/facebook-censored-54-posts-for-blasphemy-in-pakistan-in-second-half-of-2014/; Yoree Coh, *Jack Dorsey's Challenge: Simplify Twitter for Users Like Its Chairman*, Wall St. J., Oct. 22, 2015, http://blogs.wsj.com/digits/2015/10/22/jack-dorseys-new-boss-finds-twitter-intimidating-to-use/.

[68] Lorenzo Franceschi-Bicchierai, *Iran Takes Aim at Google, Wikipedia in Latest Internet Censorship Effort*, Mashable, May 16, 2014, http://mashable.com/2014/05/16/iran-google-wikipedia/.

[69] BBC, *Jokes and medicine: the Viber lives of Iranians,* Mar. 9, 2015, http://www.bbc.co.uk/monitoring/jokes-and-medicine-the-viber-lives-of-iranians

[70] Freedom House 2014, at 2.

[71] Michelle Moghtader, *Iran expands 'smart' Internet censorship*, Reuters, Dec. 26, 2014, http://www.reuters.com/article/2014/12/26/us-iran-internet-censorship-idUSKBN0K40SE20141226.

[72] Miriam Elder, *Censorship row over Russian internet blacklist*, The Guardian, Nov. 12, 2012, http://www.theguardian.com/world/2012/nov/12/censorship-row-russian-internet-blacklist.

[73] Freedom House, *Freedom on the Net 2013*, Oct. 2013, at 592, http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf.

[74] Amar Toor, *Russia banned Wikipedia because it couldn't censor pages*, The Verge, Aug. 27, 2015, http://www.theverge.com/2015/8/27/9210475/russia-wikipedia-ban-censorship.

While the site was restored, Reddit now suppresses certain posts or subsections of its site for different countries, based on requests from authorities.[75]

Brazil

In February 2015, municipal judge Luiz de Moura Correia in the state of Piauí ordered ISPs to block access to the Internet application WhatsApp in order to force WhatsApp to cooperate with local police in an investigation. This order was issued in relation to the Brazilian "Marco Civil," which authorizes a series of punishments that can be ordered against companies that do not comply with various regulations. Judge Correia's order selected the most severe of these sanctions, and interpreted it as authorizing censorship orders to ISPs."[76] Fortunately, the decision was reversed by an appellate court, citing the disproportionate impact caused by shutting down the whole service over a local investigation. Nevertheless, the prospect of blocking content or services — as opposed to other legal avenues (such as MLATs) for securing compliance with court orders — should concern USTR.

Other

The ITC's *Digital Trade in the U.S. and Global Economies, Part 2* report also listed Saudi Arabia, Egypt, Vietnam, and the United Arab Emirates as imposing substantial censorship-related barriers.[77]

As CCIA has previously stated, U.S. trade policy should ensure that insofar as any filtering or blocking is conducted against online content, policies are applied equally to both domestic and foreign websites. Furthermore, such restrictions must comply with WTO principles of transparency, necessity, being as minimally restrictive as possible, and the provision of due process to affected parties.

IV. INTERMEDIARY LIABILITY

Due to a failure to modernize liability rules in a variety of jurisdictions, foreign courts are frequently imposing substantial penalties on U.S. Internet companies for conduct that is lawful in the United States. These penalties deter direct investment and market entry by

[75] Rob Price, *Reddit is now censoring posts and communities on a country-by-country basis*, Business Insider, Aug. 14, 2015, http://www.businessinsider.com/reddit-unbanned-russia-magic-mushrooms-germany-watchpeopledie-localised-censorship-2015-8.

[76] Danny O'Brien & Katitza Rodriguez, *You Can't Block Apps on the Free and Open Brazilian Internet,* Electronic Frontier Foundation, March 2, 2015, https://www.eff.org/deeplinks/2015/03/you-cant-block-apps-free-and-open-brazilian-internet.

[77] *Digital Trade in the U.S. and Global Economies, Part 2* at 98.

multinational Internet companies, and as a consequence deny local small- and medium-sized enterprises Internet-enabled access to the global marketplace; they similarly discourage investment in and growth of domestic startups.[78] For instance, one study found that increasing liability on U.S. and EU intermediaries could decrease venture capital investments more than an economic recession. While U.S. Internet businesses have thrived domestically under carefully crafted legal frameworks, international asymmetries in liability rules frequently favor domestic plaintiffs.[79]

Below is a non-exhaustive list of countries that have imposed liability in various contexts in ways that are inconsistent with U.S. intermediary liability policy:

France

Over the years, French courts have imposed a variety of burdens on U.S. companies. In several cases, online service providers have been ruled to be ineligible for the hosting safe harbor of the E-Commerce Directive, and thus liable for users' activities (notwithstanding Directive language to the contrary) only to be overturned on appeal.[80] Similarly mixed are the outcomes of problematic French cases about search "autocompletion,"[81] as well as numerous instances of

[78] Matthew Le Merle *et al.*, *The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment: A Quantitative Study*, Booz & Co. (2011), http://static1.squarespace.com/static/5481bc79e4b01c4bf3ceed80/t/54877560e4b0716e0e088c54/1418163552585/Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

[79] For a general overview of these issues, *see* Ignacio Garrote Fernández-Díez, *Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights*, http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf (comparative analysis on national approaches to the liability of Internet intermediaries for infringement of copyright and related rights).

[80] Cour d'appel [C.A.] Paris, Feb. 4, 2011, *André Rau v. Google and Aufeminin.com*; Cour d'appel [C.A.] Paris, Jan. 14, 2011, *Google Inc. v. Bac Films, The Factory et al.*; Robert Andrews, *Google Fined In French Court For Not Stopping Video Copyright Abuse*, paidContent, Mar. 9, 2011, *available at* http://paidcontent.org/2011/03/09/419-google-fined-in-french-court-for-not-stopping-video-copyright-abuse; Tribunal de grande instance [T.G.I.] Paris, Oct. 19, 2007, *Zadig Production v. Google Inc* (Fr.); Tribunal de grande instance [T.G.I.] Paris, June 22, 2007, *Jean-Yves Lafesse v. Myspace* (reversed on procedural grounds, C.A. Paris, Oct. 29, 2008); *See, e.g.*, Cour d'appel [C.A.] Paris, Sept. 3, 2010, *LVMH v. eBay*, (*aff'g* Commercial Court Paris June 30, 2008); Cour d'appel [C.A.] Reims, July 20, 2010, *Hermes v. eBay* (*aff'g* T.G.I. Troyes, June 4, 2008); *see, e.g.*, Tribunal de grande instance [T.G.I.] Paris, Nov. 14, 2011, *Olivier Martinez v. Google and Prisma Presse*.

[81] Cour d'appel [C.A.] Paris, Dec. 9, 2009, *Google Inc v. Direct Energie*, *at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2804; Paris Tribunal de Grande Instance, Sept. 8 2010, *MX v. Google Inc, Eric S, Google France*, *at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2985. In 2011, a Paris court decided that it was possible for Google to avoid obvious infringements of personality, and thereby reasonable to impose an affirmative obligation to police content. *See* Paris Court of Appeal, Dec. 14, 2011, *Lyonnaise de Garantie v. Google France, Google Inc, Eric S.*, *at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3303 (*aff'g* T.G.I. Paris May 18, 2011, *at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3169).

French courts issuing extraterritorial orders.[82] While appellate courts have often corrected these deviations from the E-Commerce Directive, the persistent legal uncertainty poses barriers to online services' operations.

Germany

German courts have also imposed burdens on foreign defendants,[83] including orders to affirmatively monitor and filter online content, including on third-party sites,[84] which runs counter to safe harbors in the E-Commerce Directive.[85] As in some French cases, German appellate courts have corrected several of these deviations from international norms, but the uncertainty associated with lower courts' hostile approach to U.S. online services continues to be a source of business risk.

Business risk increased in Germany after the *Bundesgerichtshof's* (German Supreme Court, hereinafter 'BGH') judgment in the *Stokke* case.[86] In the *Stokke* case the BGH upheld a broad injunction, requiring an online marketplace that has booked a Google Ad linking to dynamic search results to ensure that listings displayed do not include copyright infringing content. The injunction, imposed on eBay in that case, essentially requires a manual comparison of pictures associated with new listings on a daily basis and sets a dangerous precedent that could lead to a flood of broad injunctions imposed on intermediaries in Germany.

The *Stokke* ruling directly contradicts the EU hosting liability framework, laid out in the EU E-Commerce Directive (2000/31/EC) and the IP Enforcement Directive (2004/48/EC). Article 15 of the E-Commerce Directive ensures that intermediaries do not have a general monitoring obligation to prevent infringing content from appearing on their site. This ruling,

---

[82] *Sarl Louis Feraud Int'l v. Viewfinder Inc.*, 489 F.3d 474 (2d Cir. 2007) (non-French site ordered to remove the photographs from New York servers or face penalties of 50,000 francs per day). French courts have been equally unfriendly towards Internet companies with regards to trademark liability. *See, e.g.*, Therese Poletti, *EBay Ruling in France Reeks of Protectionism*, Market Watch, July 1, 2008, http://www.marketwatch.com/story/ebay-ruling-in-france-smells-of-protectionism; Nadya Masidlover, *French Court Partly Overturns Ruling in eBay-LVMH Spat*, Wall St. J., May 3, 2012, http://online.wsj.com/article/SB10001424052702304743704577382204111836554.html.

[83] Karin Matussek, *Google Loses German Copyright Cases Over Image-Search Previews*, Bloomberg, Oct. 13, 2008, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a_C1wVkCvPww (reversed on appeal); *see also* Hamburg Regional Court, Sept. 26, 2008, *Horn v. Google*, Partial Verdict, Ref. No. 308 O 42/06; Anna Zeiter, *German Supreme Court Finds eBay Liable for Actively Promoted Third Party Copyright Infringements*, Center for Internet and Society at Stanford Law School, Dec. 18, 2013, http://cyberlaw.stanford.edu/blog/2013/12/german-supreme-court-finds-ebay-liable-actively-promoted-third-party-copyright.

[84] Ernesto, *Supreme Court Orders RapidShare to Police the Internet*, TorrentFreak, Aug. 19, 2013, http://torrentfreak.com/supreme-court-orders-rapidshare-to-police-the-internet-130819.

[85] LG Hamburg, Apr. 20, 2012, *GEMA v. YouTube*, Ref. No. 310 O 461/10; Karin Matussek, *Google's YouTube Must Help Detect Illegal Uploads, Court Says*, Bloomberg News, Apr. 20, 2012, http://www.businessweek.com/news/2012-04-20/google-s-youtube-must-help-detect-illegal-uploads-court-says.

[86] Kinderhochstühle im Internet II - I ZR 216/11; BGH.

however, imposes precisely such an obligation as it requires marketplaces to check all third party listings for potentially infringing content. In addition, the *Stokke* holding is incompatible with the judgment of the Court of Justice of the EU (CJEU) in *SABAM v Scarlet*[87] in which an injunction ordering a general monitoring obligation was declared incompatible with EU law. The CJEU subsequently confirmed this finding in *SABAM v Netlog.*[88]

Italy

Italian courts have repeatedly found international Internet companies liable in cases involving domestic plaintiffs. U.S.-based search engines have been targeted with infringement suits over third party content,[89] and have been ordered to remove links to not only websites providing infringing content, but also to other sites that *link* to potentially unlawful websites.[90] Courts in Italy are also prone to deny safe harbor protection on dubious bases.[91]

Online platforms have even been subject to criminal complaints,[92] and individual corporate employees face the risk of being sued abroad. Several years ago, Italian prosecutors criminally convicted three company executives of a U.S. Internet company, who were charged merely "because they had position of authority [sic] over the operations involved."[93] Although the conviction was ultimately overturned, for nearly three years the executives faced the prospect

[87] C-360/10 SABAM v. Scarlet.

[88] C-70/10 SABAM v. Netlog.

[89] The Finocchiaro Law Firm, *Yahoo! Announces its intention to appeal against the order of the Court of Rome*, Apr. 13, 2011, http://www.blogstudiolegalefinocchiaro.com/wordpress/2011/04/yahoo-announces-its-intention-to-appeal-against-the-order-of-the-court-of-rome.

[90] Giulio Coraggio, *Yahoo! Liable for Searchable Contents!*, DLA Piper, IPT Italy, Apr. 3, 2011, http://blog.dlapiper.com/IPTitaly/entry/yahoo_liable_for_searchable_contents.

[91] *See, e.g.*, Court of Milan, Sept. 9, 2011, *Reti Televise Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l.* One scholar noted that based on this decision, "most UGC [user-generated content] websites relying on an advertisement business models [sic] should be denied hosting protection." Béatrice Martinet Farano, *Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches* 134 (Stanford-Vienna Transatlantic Tech. Law Forum (TTLF) Working Paper No. 14, 2012), *available at* http://www.law.stanford.edu/sites/default/files/publication/300252/doc/slspublic/farano_wp14-4.pdf; Tribunale Ordinario di Milano, Mar. 24, 2011, 10847/2011, *available at* http://piana.eu/files/Ordinanza.pdf; Roland Mathys & Christoph Zogg, Wenger Plattner, *Court Denies Unlawful Infringement of Personality Through Google Suggest*, Info. Tech. (Int'l Law Office, London, U.K.), Aug. 21, 2012, *available at* http://www.internationallawoffice.com/newsletters/detail.aspx?g=0823b0fc-d75c-435e-8649-84dfd6b9fc56.

[92] Ben Wedeman, *Facebook may face prosecution over bullied teenager's suicide in Italy*, CNN, July 31, 2013, http://www.cnn.com/2013/07/31/world/europe/italy-facebook-suicide.

[93] Alessandra Galloni, *Italy Is to File Charges Against Google Executives*, Wall St. J., July 25, 2008, http://online.wsj.com/articles/SB121695694686283865; *see also* Rachel Donadio, *Larger Threat Is Seen In Google Case*, N.Y. Times, Feb. 24, 2010, http://www.nytimes.com/2010/02/25/technology/companies/25google.html?pagewanted=all.

of criminal prosecution for third-party content.[94] The availability of criminal sanctions may deter direct investment and cause both domestic and multinational enterprises to avoid deploying innovative new services.

India

While India enacted legislation to limit service provider liability in 2000 and 2008,[95] a more recent empirical study found that rules passed in 2011 have a chilling effect on free expression by encouraging over-compliance with takedown notices in order to limit liability, and by not establishing sufficient safeguards to prevent misuse and abuse of the takedown process.[96] Further demonstrating the regime's flaws, in 2012, U.S. Internet services were threatened with criminal prosecution in India for hosting material that "seeks to create enmity, hatred and communal violence" and "will corrupt minds,"[97] and executives faced possible prison terms, in addition to financial penalties,[98] based on legal standards that are essentially strict liability.[99] And while India's Supreme Court earlier clarified some sections of the 2000 IT Act, its existing provisions have still been harmful to intermediaries. In October, an administrator of a WhatsApp group was arrested when someone in his group shared a video depicting violence towards a cow and the prime minister (notwithstanding the fact that group administrators in this application cannot even delete members' posts in this app).[100] Imposing liability on an intermediary who cannot technologically respond to content is tantamount to a prohibition on use of the application.[101]

---

[94] Eric Pfanner, *Italian Appeals Court Acquits 3 Google Executives in Privacy Case*, N.Y. Times, Dec. 21, 2012, http://nytimes.com/2012/12/22/business/global/italian-appeals-court-aqcuits-3-google-executives-in-privacy-case.xml.

[95] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (Sept. 2011), at 79-80, http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm.

[96] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet* (2011), http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf.

[97] Amol Sharma, *Facebook, Google to Stand Trial in India*, Wall St. J., Mar. 13, 2012, *available at* http://online.wsj.com/article/SB10001424052702304537904577277263704300998.html.

[98] Rebecca MacKinnon, *The War for India's Internet*, Foreign Policy, June 6, 2012, *available at* http://www.foreignpolicy.com/articles/2012/06/06/the_war_for_india_s_internet?page=0,0.

[99] Amol Sharma, *In Search of Justice at the Google, Facebook Trial*, India Real Time, Mar. 13, 2012, *available at* http://blogs.wsj.com/indiarealtime/2012/03/13/in-search-of-justice-at-the-google-facebook-trial.

[100] Varun B. Krishnan, *Social Media Administrator? You Could Land in Trouble*, Oct. 10, 2015, http://www.newindianexpress.com/states/tamil_nadu/Social-Media-Administrator-You-Could-Land-in-Trouble/2015/10/10/article3071815.ece

[101] A study by Copenhagen Economics found that online intermediaries can become a significant part of India's economy and their GDP contribution may increase to more than 1.3% by 2015 provided that the existing safe harbor regime is improved. Such opportunities would be valuable to American companies. *See* Copenhagen Economics, *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Global Network

Thailand

A 2012 case in Thailand involved a criminal conviction under Thailand's Computer Crimes Act of a webmaster whose only crime was "failing to quickly delete posts considered insulting to Thailand's royal family."[102] The 2007 Computer Crime Act, while slightly amended earlier this year to exempt service providers from liability if they destroy offending data, nevertheless still contains onerous provisions under which ISPs may "be found liable for the speech of their users without a prior court order."[103]

Vietnam

A recent proposal from the Vietnamese government involved "banning people from copying and pasting news articles and other information on blogs—which could restrict the growth of informal news portals," noting that Vietnam's Communist rulers are subjected to criticism online. Government officials denied any intent to limit free speech, indicating that they aimed to "manage" growth and "protect intellectual property."[104]

Vietnam's Decree No. 55 also contains provisions which require Internet exchange providers, "...ISPs, online service providers (OSPs), ICPs, and Internet service agents to act as gatekeepers in adopting appropriate measures to block the prohibited content defined under the Press Law and the Publication Law, among others."[105] This prohibited content includes behaviors that are, in the law's words, "seditious, libelous, defamatory, obscene and violent, and those that constitute hate speech or disclose State secrets."[106]

Estonia

In June 2015, the European Court on Human Rights held that the Estonian news portal Delfi could be liable for comments posted under news articles on its site. After comments

---

Initiative, Mar. 2014, https://globalnetworkinitiative.org//sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[102] James Hookway, *Conviction in Thailand Worries Web Users*, Wall St. J., May 30, 2012, *available at* http://online.wsj.com/article/SB10001424052702303674004577435373324265632.html (noting that this "sets a concerning precedent for prosecuting website owners for what their users say online."). *See also* Center for Democracy & Technology, *Comments on Thailand's Proposed Computer-Related Offenses Commission Act*, March 2012, *available at* https://cdt.org/files/pdfs/Comments-Thailand-CCA-Draft.pdf.

[103] Jeremy Malcolm, *Intermediary Liability in Thailand Done Right and Done Wrong*, Electronic Frontier Foundation, Apr. 3, 2015, https://www.eff.org/deeplinks/2015/04/intermediary-liability-thailand-done-right-and-done-wrong

[104] James Hookway, *Vietnam Rights Record Cools U.S. Ties*, Wall St. J., Aug. 8, 2013, *available at* http://online.wsj.com/article/SB10001424127887323838204579000160962041046.html.

[105] Thuy Nguyen, *Online Intermediaries Case Studies Series: Roles and Liabilities of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear*, The Global Network of Internet & Society Research Centers (2015) at 8, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566364.

[106] *Id.* at 3.

critical of a local ferry operator featured in one article, the ferry operator asked Delfi to remove the comments. Although the portal complied after several weeks, it was nevertheless subjected to suit, and an Estonian court imposed liability on the basis of the online comments. Delfi appealed to the European Court on Human Rights, which affirmed the earlier ruling,[107] despite the fact that the portal utilizes comment filters and responded to the complaints.[108] The Delfi ruling is difficult to reconcile with more modern approaches to intermediary liability, such as 47 U.S.C. § 230 and the European E-Commerce Directive's mandated safe harbors for intermediaries, and demonstrates the dangers of holding platforms liable for third-party content. Absent suitable protection for intermediaries for liability for third party content, many U.S. services may be unable to enter foreign markets like Estonia due to the liability risks.

Finally, USTR should monitor developments regarding the Digital Single Market (DSM) communication. As part of the DSM, the European Commission has discussed the possibility of imposing a "duty of care" on Internet intermediaries, which would require Internet platforms to take a more active role in policing user content.[109] This duty of care could be effectuated by either narrowing, or completely removing, the liability safe harbors available to Internet companies under the e-Commerce Directive that have been critical to powering digital trade. Such a step would threaten the ability of U.S. Internet companies and websites to serve users in the 28 European Member States, and impair the ability of online platforms to serve as conduits for trade, including by the small businesses that have become 'micro-multinationals' through the Internet.

V. COPYRIGHT LIMITATIONS AND EXCEPTIONS

Balanced copyright rules such as fair use and related limitations and exceptions have been critical to the growth of the U.S. technology and Internet economy. As Judge Pierre Leval

[107] Mark Scott, *Estonian News Site Can Be Held Liable for Defamatory Comments, Court Rules,* N.Y. Times, June 17, 2015, http://www.nytimes.com/2015/06/18/business/media/estonian-news-site-can-be-held-liable-for-defamatory-comments-court-rules.html; *see also* Heather Greenfield, *European Court Rules Online News Sites Liable For Online Comments*, CCIA News, Jun. 17, 2015, http://www.ccianet.org/2015/06/european-court-rules-online-news-sites-liable-for-online-comments/.

[108] Mike Masnick, *Huge Loss For Free Speech In Europe: Human Rights Court Says Sites Liable For User Comments*, Techdirt, June 16, 2015, https://www.techdirt.com/articles/20150616/11252831361/huge-loss-free-speech-europe-human-rights-court-says-sites-liable-user-comments.shtml.

[109] *See* James Waterworth, *European Commission Releases Digital Single Market Strategy: The Good and the Bad*, Disruptive Competition Project, May 6, 2015, http://www.project-disco.org/competition/050615-europes-digital-single-market-strategy-the-good-and-the-bad/.

wrote in an influential 1990 Harvard Law Review article, "Fair use should not be considered a bizarre, occasionally tolerated departure from the grand conception of the copyright monopoly. To the contrary, it is a necessary part of the overall design."[110] Within the last thirty years, such rules have enabled the development of innovative new products and services such as the VCR, DVR, iPod, cloud computing, search engines, social media services, and 3D printing. Similarly, users of copyrighted works—including consumers, libraries, museums, reporters, and creators—depend upon concepts like fair use and other limitations and exceptions to engage in research, reporting, parody, and political discourse.

These innovations are jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of other countries. For example, as CCIA observed in its previous NTE submission, legislatures in Europe and elsewhere have increasingly proposed or implemented new publisher subsidies styled as so-called "neighboring rights" – related to copyright – that may be invoked against online news search services. U.S. and other providers of online search, news aggregation, and social media platforms are compelled to pay for the "privilege" of quoting from news publications. This proposal is often referred to as a quotation or snippet tax. It is at times formally described as an "ancillary" IP right, but it is in fact inconsistent with international IP law, violates international trade obligations, and constitutes a TRIPS-violating barrier to trade.

As CCIA commented in the 2015 Special 301 proceedings,[111] restrictions on the quotation right violate international obligations. Article 10(1) of the Berne Convention provides: "It *shall be* permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries."[112] Thus, established international

---

[110] Pierre Leval, *Toward a Fair Use Standard*, 103 Harv. L. Rev. 1105, 1110 (1990).

[111] Comments of CCIA, Dkt. No. USTR-2014-0025, filed Feb. 6, 2015, at 2-6, *available at* http://cdn.ccianet.org/wp-content/uploads/2015/02/CCIA-Special-301-Comments-2015.pdf. *See also, e.g.*, Comments of CCIA, Dkt. No. USTR-2010-003, filed Feb. 16, 2010, at 5, *available at* http://cdn.ccianet.org/wp-content/uploads/2015/02/CCIA-Special-301-Comments-2015.pdf (explaining that Berne-related TRIPS violations are germane to § 2242(a)(1), possibly necessitating identification as 'acts, policies, or practices' having actual or potential impact on relevant United States products."); *see also* Comments of CCIA, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013, at 11-12, *available at* http://www.ccianet.org/wp-content/uploads/library/CCIA%20Comments%20on%20Special%20301%20[2013].pdf ("By virtue of Berne's incorporation in TRIPS, Article 10(1) imposes a mandatory, affirmative obligation on WTO Members to permit anyone to quote from a work that is already lawfully publicly available").

[112] Berne Convention for the Protection of Literary and Artistic Works, art. 10(1), amended Oct. 2, 1979 (emphasis supplied).

copyright rules prohibit nations from restricting the right to quote. Because this provision of Berne is incorporated in TRIPS,[113] WTO Members have a mandatory, affirmative obligation to permit anyone to quote from a work that is already lawfully publicly available. An ancillary right or any other form of snippet tax would abrogate this right in violation of TRIPS obligations. Policymakers across Europe, in national capitals and Brussels, have expressed interest in establishing these TRIPS-inconsistent entitlements as a vehicle to tax services exported by American Internet companies.[114] At present, laws in Spain and Germany pose the most significant barriers to U.S. exporters.

Germany

In August 2013, Germany's ancillary copyright law (*Leistungsschutzrecht*) took effect, extending copyright protection to snippets, i.e. small text excerpts in search results, which violates international obligations that require free quotation.[115] This statute expressly holds search engines liable for making available to the public snippets in search results, thereby creating direct liability for the automatic processes by which search results are generated. CCIA and others have argued that this statute is inconsistent with Germany's international obligations. In addition to representing a trade barrier, the statute has also been the subject of a challenge under German constitutional law.[116]

During the drafting of the statute, a late change excluded "smallest text excerpts" from the scope of the law, creating some uncertainty as to what that term meant. In September 2015, the German Copyright Arbitration Board suggested that if the length of such 'snippets' exceeds seven words (excluding 'keywords'), then search engines and other news aggregators should be

[113] TRIPS Agreement, art. 9 ("Members shall comply with Articles 1 through 21 of the Berne Convention (1971)").

[114] *EU's Oettinger mulls levy on Google - Handelsblatt*, Reuters, Oct. 28, 2014, http://www.reuters.com/article/2014/10/28/eu-commission-oettinger-idUSL5N0SN34020141028; *Oettinger Floats Proposal for EU-wide 'Google-tax'*, EurActiv, Oct. 29, 2014, http://www.euractiv.com/sections/innovation-enterprise/oettinger-floats-proposal-eu-wide-google-tax-309568; *EU plant Urheberrechtsabgabe im Internet*, Handesblatt, Oct. 28, 2014, http://www.handelsblatt.com/politik/international/schutz-geistigen-eigentums-bis-2016-eu-plant-urheberrechtsabgabe-im-internet/10900130.html ("…Wenn Google intellektuelle Werte aus der EU bezieht und damit arbeitet, dann kann die EU diese Werte schützen und von Google eine Abgabe dafür verlangen").

[115] *See generally* Comments of CCIA, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013, *available at* http://www.ccianet.org/wp-content/uploads/library/CCIA%20Comments%20on%20Special%20301%20[2013].pdf.

[116] Loek Essers, *German copyright law is unconstitutional, Yahoo says in complaint*, PCWorld (Aug. 1, 2014), http://www.pcworld.com/article/2460720/german-copyright-law-is-unconstitutional-yahoo-says-in-complaint.html (explaining Yahoo's claim that the law conflicts with the German constitutional protections to freedom of information and from government action restricting access to information).

liable for the "snippet tax."[117] If a court confirmed this suggestion, the law would clearly be inconsistent with U.S. copyright norms as well as Berne.[118]

Notably, efforts to adjust practices to account for the law proved unsuccessful. Even as some news publishers offered a limited license to Google to show snippets,[119] they filed a complaint with the German competition authority arguing that Google was abusing its position for choosing not to show snippets. (Authorities later rejected the complaint, ruling that Google cannot be compelled to possibly adopt liability in a case where "the legal situation is unclear".)[120]

Spain

As discussed more fully in CCIA's 2015 Special 301 submission,[121] the Spanish partial reform of intellectual property laws instituted a similar "snippet tax" that violate Spain's international commitments by subjecting normal quotations to a form of levy. The Spanish law modified the German approach by prohibiting news producers from waiving their right compensation, such that there is no means by which a covered news creator can waive rights or license platforms to publish snippets. Faced with this measure, Google suspended its Google News service in the Spanish market. An economic consultancy found that, as a result of Google News shutting down in Spain, web traffic to smaller publications declined by about 14%, more than double the average traffic decline.[122] Such measures hardly help Spanish consumers either. Since news aggregators are discouraged under this law, there are fewer paths for people to find news published by smaller publications with less brand recognition. Like the German *Leistungsschutzrecht*, the Spanish IP revision not only undermines market access for U.S.

---

[117] Jennifer Baker, *You want a 6% Google Tax? Get lost, German copyright bods told: Only snippets longer than seven words are chargeable*, The Register, Sept. 28, 2015, http://www.theregister.co.uk/2015/09/28/google_tax_6_pe_cent_germany_fails/.

[118] *See, e.g.*, *Faulkner Literary Rights v. Sony Pictures Classics*, 953 F. Supp. 2d 701 (N.D. Miss. 2013) (finding quotation of nine words to be non-infringing). *See also* CCIA White Paper, *Understanding 'Ancillary Copyright' in the Global Intellectual Property Environment*, at 5-6, *available at* http://cdn.ccianet.org/wp-content/uploads/2015/02/CCIA-Understanding-Ancillary-Copyright.pdf (February 2015) (explaining Berne authors rejection of requirement that quotations be "short").

[119] Greg Sterling, *German Publishers To Google: We Want Our Snippets Back*, Search Engine Land, Oct. 23, 2014, http://searchengineland.com/german-publishers-google-want-snippets-back-206520.

[120] Bundeskartellamt News, *Bundeskartellamt takes decision in ancillary copyright dispute,* Sept. 9, 2015, http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2015/09_09_2015_VG_Media_Google.html?nn=3591568.

[121] *See supra* note 112.

[122] NERA Econ. Consulting, *Impacto del Nuevo Artículo 32.2 de la Ley de Propiedad Intelectual*, xi, July 9, 2015, http://www.nera.com/content/dam/nera/publications/2015/090715%20Informe%20de%20NERA%20para%20AEEPP%20(VERSION%20FINAL).pdf.

companies and distort established copyright law, but it also violates the EU and Spain's treaty and WTO commitments.[123]

VI. OTHER RESTRICTIONS ON MOVEMENT OF OR ACCESS TO INFORMATION

A. EU-U.S. Safe Harbor Developments

The recent ruling by the Court of Justice of the European Union (CJEU) invalidating the European Commission's adequacy determination for the EU-U.S. Safe Harbor framework has led to considerable regulatory uncertainty for companies with transatlantic operations. The Safe Harbor program allowed for thousands of companies (including U.S. subsidiaries of European companies) to transfer data relating to EU citizens who use their services. USTR said of Safe Harbor in last year's NTE: "The United States actively supports Safe Harbor and will work to ensure that it remains available to support transatlantic data flows, which are vital to both the U.S. and EU economies and continues to serve all stakeholders well."[124]

Since its inception, the Safe Harbor has been a primary vehicle through which authorities certified that transatlantic companies respect EU data protection principles. In the aftermath of the CJEU ruling, companies are now concerned about continuing to transfer data absent consistent guidance about the ruling from the EU Commission and data protection authorities. In the wake of the CJEU's decision, EU data protection authorities, through the Article 29 Working Party, have indicated that enforcement of EU-wide data protection requirements will begin at the end of January 2016. However, this guidance does not provide sufficient answers to ensure that companies do not find themselves in breach of EU law when transferring data from Europe to the United States even if such transfers are necessary for business operations.[125]

The currently available alternatives to permit EU-compliant data transfers are complex legal mechanisms, including binding corporate rules and standard contract clauses.[126] Both

---

[123] *See* Raquel Xalabarder, *The Remunerated Statutory Limitation for News Aggregation and Search Engines Proposed by the Spanish Government - Its Compliance with International and EU Law*, IN3 Working Paper Series (Sept. 30, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504596.

[124] Office of the Unted States Trade Representative, *2015 National Trade Estimate Report on Foreign Trade Barriers*, 2015, https://ustr.gov/sites/default/files/2015%20NTE%20Combined.pdf.

[125] *Statement of the Article 29 Working Party,* Oct. 16, 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[126] Even this option is not necessarily guaranteed in all EU member states; a recent conference of German data protection authorities (comprising the federal and state DPAs) released a paper taking the position that binding corporate rules would not serve as a basis for new approvals of data transfers. *See* Michelle Gyves, *German DPAs Announce Policy Severely Limiting Mechanisms for Lawful Germany-to-U.S. Data Transfers,* Proskauer Privacy

options are costly, piecemeal, require time for approval, and are difficult to implement for even the most sophisticated companies. Expecting small- and medium-sized enterprises to successfully adopt these alternatives, particularly in the short term, to comply with the varying requirements of the data protection authorities of each EU member state would seem unlikely. Moreover, these alternative mechanisms may also be called in question by future regulators, just as the Safe Harbor was. Forcing international companies to store all personal data in Europe is not feasible and would hit small firms the hardest. Significant penalties may be associated with the enforcement of these rules: under new regulations being considered, European national data protection authorities may be empowered to fine companies up to 2% of global annual turnover.[127]

B. "Right to be Forgotten"

Last year's ruling by the CJEU on the "Right to be Forgotten" requires search engine operators to delist URLs from their search results at the request of individuals in the EU, if the website is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed."[128] In the year that the CJEU ruling has been in effect, a lack of consistent guidance has raised concerns for companies with global consumer bases. Those concerns result from uncertainty about how the ruling affects search providers' ability to provide accurate information to users and the possible extraterritorial application of the ruling by EU national data protection authorities.

For example, some search engines have been instructed that they should not link to certain news stories about the ruling in their search results, since those stories may refer to individuals who had earlier successfully petitioned for 'the right to be forgotten.' In August 2015, the UK's data protection authority ordered the removal of links to ". . . current news stories about older reports which themselves were removed from search results under the 'right to be forgotten' ruling."[129]

Law Blog, Oct. 26, 2015, privacylaw.proskauer.com/2015/10/articles/european-union/german-dpas-announce-policy-severely-limiting-mechanisms-for-lawful-germany-to-u-s-data-transfers/.

[127] European Commission Press Release, *Stronger Data Protection Rules for Europe*, June 15, 2015, *available at* http://europa.eu/rapid/press-release_MEMO-15-5170_en.htm.

[128] Court of Justice of the European Union, *Press Release No 70/14,* May 13, 2014, *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

[129] Samuel Gibbs, *Google ordered to remove links to 'right to be forgotten' removal stories*, The Guardian, Aug. 20, 2015, http://www.theguardian.com/technology/2015/aug/20/google-ordered-to-remove-links-to-stories-about-right-to-be-forgotten-removals.

Other authorities have asserted that search engines must erase links from *all* domains used by the company, even though they may be focused on international audiences. For example, the French Data Protection Authority (CNIL) recently mandated that Google must apply 'right to be forgotten' search result removals not just to searches on the .fr or .co.uk domains, but also to those conducted on .com and other Google domains with worldwide reach. Effectively, French authorities sought to constrain what non-French Internet users would be able to access under EU legal standards.[130] CNIL could fine Google roughly €300,000 for refusal to comply, and under proposed European regulations the fine could increase to between 2% and 5% of global operating costs.[131]

Putting the onus on companies to respond to all requests in compliance with the 'right to be forgotten' ruling is administratively burdensome. For example, Microsoft has fielded thousands of requests in the first half of 2015 alone,[132] and Google has fielded more than 300,000 requests since the policy went into effect.[133] Processing these requests requires considerable resources since each must be examined individually. Small- and medium-sized enterprises who also offer similar services but without the resources to field these requests could find that this ruling poses a barrier to entry into the EU. USTR should monitor the outcome of this ruling for adherence with international commitments.

VII. UNDUE RESTRICTIONS ON OVER-THE-TOP SERVICES

Several countries have proposed or implemented undue or unreasonable regulatory restrictions on Over-The-Top (OTT) services.

For example, in October 2014, Vietnam's government released a draft "Circular on Managing the Provision and Use of Internet-based Voice and Text Services" that proposed unreasonable restrictions on VoIP and Internet Based Text Services provided over IP broadband connections. These restrictions would require foreign providers of OTT services to install a local server to store data or enter into a commercial agreement with a Vietnam licensed

[130] Greg Sterling, *Right To Be Forgotten: French Argue They Have Authority To Regulate Google Globally,* Search Engine Land, Sept. 21, 2015, http://searchengineland.com/right-to-be-forgotten-french-argue-they-have-authority-to-regulate-google-globally-231233.

[131] Samuel Gibbs, *French data regulator rejects Google's right-to-be-forgotten appeal*, Guardian, Sept. 21, 2015, http://www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal.

[132] Microsoft, *Content Removal Requests Report*, http://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/crrr/.

[133] Google, *European privacy requests for search removals*, http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en.

telecommunications company. In addition, foreign providers of OTT services would only be permitted to place a server in Vietnam through cooperation with Vietnam's telecommunications companies. Such requirements are significant market access barriers for foreign competitors that seek to supply Internet-based services in Vietnam, and may be designed to raise the costs of rivals providing service in Vietnam.

Other jurisdictions are considering similar regulations. In India, the Telecommunications Regulatory Authority and the Department of Telecommunications have proposed introducing licensing and regulatory obligations targeted at OTT VoIP. In the European Union, there have been discussions about using regulations to "level the playing field" and correct for supposed market advantages of OTT services, most recently in the European Commission's review of the Audiovisual Media Services Directive and potentially in the Digital Single Market proceeding as well.

USTR should encourage these and other countries that may be considering similar regulations—such as Myanmar and Pakistan—to promote policies to encourage greater growth and competition in ICT services. OTT services help drive growth in some of the most profitable services offered by telecommunications providers.[134] In addition, OTT services also present cost-saving and product-enhancement opportunities for telecom providers, such as the opportunity to substitute fully featured VoIP for circuit-switched voice.

VIII. CONCLUSION

As the global Internet continues to grow and becomes even more tightly intertwined with international commerce, CCIA worries that – if left unchecked – digital trade barriers like those discussed above will continue to promulgate. To help push back against these barriers, U.S. trade policy and enforcement priorities need to be updated to reflect the large and growing importance of the Internet to the U.S. economy and U.S. trade performance.

Furthermore, as numerous studies have pointed out,[135] Internet platforms and services empower small- and medium-sized businesses to participate in international trade like never

[134] *See* OECD, *The Development of Fixed Broadband Networks* (Jan. 2015), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP%282013%298/FINAL&docLanguage=En (noting that "pricing mechanisms that do not excessively depress demand have the advantage of stimulating adoption").

[135] *See, e.g.*, Andreas Lendle, *et al*., *There Goes Gravity: How eBay Reduces Trade Costs*, The World Bank Poverty Reduction and Economic Management Network International Trade Department, Oct. 2012, http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/10/25/000158349_20121025161729/Rendered/PDF/wps6253.pdf; *see also Internet Matters*, *supra* note 10.

before. Small businesses and individual craftsmen can use platforms like eBay and Etsy to sell their wares globally without the need of an international presence. Payment processors like PayPal and Google Wallet allow the same firms to process payments globally (provided local financial regulations allow for it), and global Internet advertising networks like those offered by Facebook, Twitter, Google and Amazon allow these companies and individual sellers to target potential customers across borders. Therefore, positive efforts on the digital trade front will also expand the base of U.S. exporters (and foreign exporters) that directly benefit from U.S. trade policy.