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

In re	
Request for Public Comments on Compliance with Telecommunications Trade Agreements	Docket No. USTR-2014-0022

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 79 Fed. Reg. 66,446 (Nov 7, 2014), the Computer & Communications Industry Association (CCIA) submits the following comments for consideration as the USTR composes its Section 1377 Review of Compliance with Telecommunications Trade Agreements report.

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 600,000 workers and generate annual revenues in excess of $465 billion.

As a cross-sectoral high-tech trade association, our members face many different obstacles to conducting international commerce over telecommunications networks. As the Internet continues its vigorous growth and becomes a central component of cross-border trade of both goods and services, removing barriers to Internet-enabled trade becomes imperative. Given the U.S.'s leadership in high-tech innovation and Internet technology, clearing hurdles to the export of Internet-enabled products and services over telecommunications networks promises huge economic gains, as the U.S. International Trade Commission (ITC) made clear in a recent report:

> Products and services delivered via the Internet make up a growing segment of the U.S. economy. Internet technologies have also transformed how many goods and services in the economy are produced and delivered. Digital sales make up more than half of music industry revenue; the digital shares of sales for games, videos, and books are smaller, but growing quickly. U.S. exports of digitally enabled services (one measure of international digital trade) grew from $282.1 billion in 2007 to $356.1 billion in 2011, with exports exceeding imports every year. Studies 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.[1]

For major U.S. Internet companies, international markets have become increasingly more important and the potential for international competition has become more robust. The latest installment of noted industry analyst Mary Meeker's annual report on Internet trends documents this phenomenon. While nine out of the top ten "global Internet properties" are made in the U.S., 79% of their users come from outside the U.S.[2] Compare this to 2005, when Google's total international revenue was 39% of its overall sales.[3] Now, 56% of Google's revenue comes from overseas.[4] For Facebook, it is a similar story. Currently, 86% of Facebook's users are international,[5] while less than 50% of Facebook users were international as of 2008.[6] As these examples illustrate, access to international markets will be increasingly vital going forward if the U.S. Internet economy is to continue its robust growth.

With this in mind, CCIA focuses its comments on several key obstacles to Internet-enabled trade in services, including infrastructure localization mandates, the filtering and blocking of Internet content, and onerous intermediary liability regimes.

Government restrictions that serve to block or impede information flows online, whether through direct blocking, infrastructure localization mandates, or onerous liability rules, essentially restrict access of Internet service providers to the telecommunications networks themselves. Such actions can run afoul of commitments made under the GATS Telecommunications Annex, where WTO members have recognized that telecommunications networks serve as a "mode of transport" for the provision of services. In service sectors where members made liberalization commitments, they are also required to allow foreign service suppliers reasonable and non-discriminatory access to their public telecommunications networks. Finally, some of these restrictions run counter to our trade partners' other telecom-related services commitments.

---

[1] United States International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1* (July 2013), *available at* http://www.usitc.gov/publications/332/pub4415.pdf.

[2] Mary Meeker, *Internet Trends 2014*, at 130, *available at* http://www.kpcb.com/internet-trends.

[3] Press Release, Google, Google Announces Fourth Quarter and Fiscal Year 2005 Results, Jan. 31, 2006, *available at* https://investor.google.com/earnings/2005/Q4_google_earnings.html.

[4] Press Release, Google, Google Announces Fourth Quarter and Fiscal Year 2013 Results, Jan. 30, 2014, *available at* http://investor.google.com/earnings/2013/Q4_google_earnings.html.

[5] Cooper Smith, *7 Statistics About Facebook Users That Reveal Why It's Such A Powerful Marketing Platform*, Business Insider, Nov. 16, 2013, *available at* http://www.businessinsider.com/a-primer-on-facebook-demographics-2013-10.

[6] Miguel Helft, *Facebook Makes Headway Around the World*, N.Y. Times, July 7, 2010, *available at* http://www.nytimes.com/2010/07/08/technology/companies/08facebook.html.

II. DATA AND INFRASTRUCTURE LOCALIZATION

The Internet's rapid growth depends upon its end-to-end design, allowing heterogeneous hardware to be attached to the edges of the network and immediately send and receive data to any other 'node' of the network. At the same time, the network is also designed to ensure that packets of data take the most efficient route between two points. These features undergird the resilience, reliability and flexibility of the Internet, but run contrary to the desires of some governments seeking jurisdictional control, political leverage, and/or local investment from online services. As a result, policies mandating local infrastructure as a pre-condition to operating locally have become attractive to certain jurisdictions. To date, data and digital-infrastructure localization requirements have taken many different forms, including requiring the use of a local top level domain, requiring servers or people be located within a country to provide service domestically, and mandating that all data on a country's citizens be stored locally. Some countries such as Russia, Nigeria and Indonesia have gone as far as requiring all data on its citizens to be stored and processed locally, which would not only require redundant data centers and personnel, but would also present numerous logistical problems associated with decentralizing expertise and artificially segmenting data analysis.

In recent years, there has been an unfortunate increase in countries imposing or considering imposing data and infrastructure localization requirements upon companies seeking to provide digital services within a country or to a country's citizens. Efforts to impose localization requirements have accelerated after the Snowden revelations of widespread electronic spying by U.S. intelligence agencies. Stated motivations for these policies include the desire to ensure domestic privacy protections, to protect against foreign spying, to ensure law enforcement access to data, and to promote local economic development.

As political responses, the desires behind localization policies are understandable. However, data localization requirements would work contrary to stated goals of the policymakers who have proposed and implemented them.

Ensuring local data storage and processing does little to ensure user privacy and data security. In fact, unnecessarily scattering digital infrastructure around the world creates a host of new targets of opportunity for hackers, criminals and foreign intelligence agencies. Making matters worse, regulations that require all citizen data to be stored in a local data center often work against data security best practices. For example, "sharding" – the process of scattering pieces of encrypted data in multiple data centers around the world so an intrusion into one data center would not

compromise individual data – would be made difficult for large companies and impossible for smaller companies. As Pranesh Prakash, Policy Director with India's Centre for Internet and Society points out, "The correct solution would be to encourage the creation and use of de-centralised and end-to-end encrypted services that do not store all data in one place."[7] Furthermore, some countries that have or are considering data localization requirements are hotbeds for digital criminal activity, including Indonesia, Brazil, Vietnam and Russia. Given that the most common threats to individual data involve data breaches by hackers against insecure IT systems, creating a network of more numerous and insecure data centers that will also serve as full repositories for all the data of a given nation's citizens will create a wealth of new targets of opportunity for those wishing to access information for nefarious purposes.[8]

Moreover, localizing data within individual countries will do little to guard against the threat of foreign intelligence agency access to that data. Often foreign surveillance is done through collection abroad and the use of malware that can operate beyond a country's borders. Compounding the problem, to the extent countries have checks on the activities of their intelligence agencies, they are usually applied only to the domestic gathering of data and intelligence. Insofar as law enforcement access to information is a driving issue behind localization requirements, they will likely be ineffective as localization requirements are notoriously difficult to enforce. As a result, criminal or terrorist elements will simply migrate to using less compliant and more secretive services and away from those providers that are compliant with domestic wiretapping regimes.[9]

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. As the McKinsey Global Institute documented, 75% of the value of the Internet accrues to traditional, non-Internet centric businesses through productivity gains and easier access to foreign markets.[10] As a result, such policies will invariably harm a wide swath of the traditional domestic economic activity and harm a country's global competitiveness. Given the high cost of constructing data centers (i.e. the average cost of data centers in Brazil and Chile, as examples, are $60.3 million

[7] Rohin Dharmakumar, *India's Internet Privacy Woes*, Forbes India, Aug. 23, 2013, *available at* http://forbesindia.com/article/checkin/indias-internet-privacy-woes/35971/1.

[8] 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, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858 (hereinafter "Chander & Le").

[9] *Id.* at 43-46.

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

and $43 million, respectively)[11], many companies will simply opt out of serving markets with onerous data localization requirements. This holds especially true for small- and medium-sized businesses. Furthermore, as tools for local job creation, these measures do little as data centers are populated by thousands of computers and relatively few humans. Approximately three-quarters of the cost of operations of a data center is energy related and the majority of initial capital spending is devoted to importing IT products from abroad.[12] It is not surprising that a group of 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 thinking about adopting, them.[13]

As such, data localization requirements run afoul of global trade norms where trade-restrictive measures are supposed to be limited to policies that are both necessary for achieving a legitimate national security or public policy objective and the least trade restrictive method possible for achieving that desired policy outcome. In addition, these regulations are often vaguely construed, inadequately articulated and, therefore, nearly impossible to effectively implement.[14]

Below is a non-exhaustive list highlighting a few examples of current trade-restrictive policies or policy proposals:

Russia

Localization measures were signed into law in July of 2014, requiring all operators of personal data to use databases stored exclusively in Russia and to disclose the address of these databases. There is also an effort to move the original deadline for compliance of September 1, 2016 up over a year to January 1, 2015.[15]

India[16]

The 2011 amendments to the Information Technology Act of 2000 restrict the transfer of data to cases only "if it is necessary for the performance of the lawful contract" or when the data

[11] Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, Wall St. J., Nov. 13, 2013, *available at* http://online.wsj.com/articles/SB10001424052702304868404579194290325348688.

[12] Chander & Le at 37.

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

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

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

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

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 agencies to host their website on servers within India, and to restrict use of private services regardless of geographic origin. Recent disclosures suggest that localization policies will soon extend to non-government communications as well, requiring all private data of Indian citizens be stored on servers within the country and preventing the mirroring of data on servers abroad.

Nigeria

The Federal Ministry of Communications and Technology launched guidelines for Nigerian content development on IT platforms, as part of the 2007 NITDA[17] Act. Ambiguously written, it is being positioned as a framework to further enable and boost Nigeria's economy by way of infrastructure localization (including data, technology, content, etc.). Announced in December 2013, the guidelines include a requirement for a local development plan for the creation of jobs, recruitment of local engineers and the development of hardware locally. There are many problematic sections including the requirement to host all subscriber and consumer data within the country and to host all government data locally unless an official exemption is granted. Furthermore, companies must obtain 80% of all services from local Nigerian companies. Multinational companies must comply with the law within two years.

China

The Chinese government has 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

[17] National Information Technology Development Agency (NITDA) is generally perceived as an institution that is seeking relevance after largely being sidelined in the last ten years of ICT development in Nigeria. *See* http://www.nitda.gov.ng.

Chinese firms if they wish to conduct business within China[18] 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.[19]

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.*"[20] Furthermore, the French government's cybersecurity agency has proposed guidelines for cloud computing that include forced data localization.[21]

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 (even if the usage is in compliance with the EU-U.S. Safe Harbor).[22]

Germany

France's efforts regarding localization have been mirrored in Germany along with calls for a European data network.[23] 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 Germany", which routes data only through domestic servers.[24] The German government has also announced their plans to stop international data transfers until they were assured of compliance with data protection laws of foreign intelligence services.[25] 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.

---

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

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

[20] Chandler & Le at 11-12.

[21] *Appel public à commentaires sur le référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage*, Aug. 11, 2014, *available at* http://www.ssi.gouv.fr/fr/menu/actualites/appel-commentaires-referentiel-d-exigences-informatique-nuage.html.

[22] Chander & Le at 12-13.

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

[24] Michael Birnbaum, *Germany looks at keeping its Internet mail traffic inside its borders*, Wash. Post, Nov. 1, 2013, *available at* 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.

[25] Chander & Le at 14.

Hungary

In October 2014, the Hungarian government introduced a tax on Internet traffic, which would have serious consequences for the ability to access information. The European Commission criticized the tax, which would be implemented in the 2015 tax code.[26] Although the Hungarian government backed away from its initial plan after mass protests and criticism from telecommunications and technology firms, Hungary's Prime Minister stated that he would like to revive the proposal next year after consulting with various stakeholders.[27]

Brazil

While proposed language requiring all companies to store local users' data within the country was removed, legislation has recently passed that will hold U.S. companies subject to Brazilian law in cases concerning information on Brazilians, even if the data is stored outside the country.[28]

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.[29]

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.[30] This law has been accompanied by numerous burdensome regulations the local server 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

[26] Nikolaj Nielson, *EU commission lashes out at Hungary's internet tax plan*, EUobserver, Oct. 29, 2014, *available at* http://euobserver.com/justice/126294/.

[27] Margit Feher, *Hungary Drops Internet Tax Plan For Now,* Wall St. J., Oct. 31, 2014, *available at* http://online.wsj.com/articles/hungary-drops-internet-tax-plan-1414744757.

[28] Anthony Boadle, *Brazil to drop local storage rule in Internet bill*, Reuters, Mar. 18, 2014, *available at* http://www.reuters.com/article/2014/03/19/us-brazil-internet-idUSBREA2I03O20140319.

[29] Chander & Le at 19-20.

[30] *Id.* at 23.

local resident.[31] 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.

III. FILTERING AND BLOCKING

The development of the Internet has led to a revolution in the way international commerce and trade is conducted. In the new world of electronic commerce, removing obstacles and helping trade flow as freely as possible means safeguarding the free flow of information. Restrictions on that flow have grave consequences for U.S. Internet companies. However, governments are increasingly filtering and blocking Internet content, platforms and services for moral and security reasons. Whether for political or economic considerations, and 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 very harmful for the service in question; content providers, advertisers and any other businesses using the service to interact with customers are immediately affected.

The United States is an information economy, and U.S. companies are leading vendors of information products and services. In this context, information discrimination by foreign governments fundamentally undermines U.S. economic interests. Filtering American Internet content and services has the effect of filtering out American competition, and it must be combated. When governments restrict the Internet, it creates a hostile market environment by preventing consumers from fully using new products, applications and services offered by or through U.S. technology companies.

The OpenNet Initiative (ONI) has found that 42 countries have engaged in some form of filtering of content, while 21 have engaged in "substantial" or "pervasive" filtering.[32] At times the motivation for censorship is self-evident, or is disclosed, but generally the processes and reasons for censoring Internet services and content are opaque. With few exceptions, states do not attempt to justify blocking or unblocking Internet content or services, and restrictions are not developed in a transparent manner. The lack of clarity in the censorship rules is sometimes used against foreign

[31] *Id.* at 24.

[32] *Global Internet Filtering in 2012 at a Glance*, Apr. 3, 2012, *at* https://opennet.net/blog/2012/04/global-internet-filtering-2012-glance.

firms and to the advantage of domestic ones.[33] The motivation for these practices may be political, or it may be economic, but regardless, censorship constitutes a substantial barrier to digital trade in the global economy. Known offenders include Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran, Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.

Censorship methods vary, but generally consist of (a) legal or regulatory obligations imposed upon intermediary services, (b) blocking and/or filtering executed at the network level through state control or influence over the communications infrastructure, or (c) technology mandates that either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology or back-doors. Examples of legal and regulatory requirements imposed upon Internet services include blocking access to an entire Internet service or specific keywords, web pages, and domains; requiring Internet search engines to disappear search results; and demanding service providers take down certain web sites.

Perhaps the most apparent barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content. Freedom House found that 29 countries "have used blocking to suppress certain types of political and social content."[34] The trade costs of filtering are both direct and indirect. When a website or platform, such as YouTube or WordPress, is directly blocked, the trade distorting effects are obvious. However, filtering also impedes digital exports indirectly. When countries operate 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.[35]

Below are several countries with problematic blocking and filtering that restricts trade:

China

High-profile examples of targeted blocking of whole services include China's blocking of major U.S. websites including Facebook, Picasa, Twitter, Tumblr, Google+, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare.[36] AmCham China's 2013 Business Climate Survey

---

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

[34] Freedom House, *Freedom on the Net 2013*, Oct. 2013, at 3, *available at* http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf.

[35] *See* Paul Mozur & Carlos Tejada, *China's 'Wall' Hits Business*, Wall St. J., Feb. 13, 2013, *available at* http://online.wsj.com/articles/SB10001424127887323926104578277511385052752.

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

found that 55% of U.S. companies doing business in China see Internet restrictions as negatively affecting their capacity to do business there, while 62% said search engine disruption made it more difficult to obtain market data, share information, or collaborate with colleagues.[37]

Turkey

At various times Turkey has blocked popular websites, including Twitter and YouTube,[38] having adopted laws in February "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.'"[39] Turkey's telecommunications firms have even impersonated U.S. companies' servers to block access to social-media sites.[40]

Iran

In May, Iran blocked access to Google's hosting platform, Google Sites, and censored at least two Wikipedia pages.[41]

Russia

Russia's 2012 Internet blacklist law, depending how expansively it is used, has the potential to block numerous American owned websites and services.[42] According to Freedom House, "(b)locking 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."[43]

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.[44]

Although it is not feasible to prohibit all instances of Internet filtering and blocking, such

---

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

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

[39] Reporters Without Borders, *Turkey, Enemy of the Internet?*, Aug. 28, 2014, *available at* http://en.rsf.org/turquie-turkey-enemy-of-the-internet-28-08-2014,46856.html.

[40] Emre Peker, Joe Parkinson & Sam Schechner, *Google, Others Blast Turkey Over Internet Clampdown*, Wall St. J., Apr. 1, 2014, *available at* http://online.wsj.com/articles/SB10001424052702303978304579473190997035788.

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

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

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

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

instances should be kept to an absolute minimum. Websites and services should not be blocked unless a high-bar test of necessity is met. If it is met, that bar should apply equally to both domestic and foreign websites. Furthermore, such restrictions should be required to 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

U.S. businesses continue to face challenges when engaging in international, Internet-enabled trade of services over telecommunications networks. 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 multinational Internet companies, and as a consequence deny local small- and medium-sized enterprises Internet-enabled access to the global marketplace; they similarly discourage domestic startups.[45] 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.[46]

Below is a non-exhaustive list of countries that have imposed liability in various contexts in ways that are inconsistent with the EU's E-Commerce Directive safe harbor and U.S. intermediary liability policy generally:

France

Over the years, French courts have proven hostile to 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.[47] Similarly mixed are the outcomes of problematic

[45] Matthew Le Merle et al, *The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment: A Quantitative Study*, Booz & Company (2011), *available at* http://www.booz.com/media/uploads/BoozCo-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

[46] For a general overview of this issues, *see* Ignacio Garrote Fernández-Díez, *Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights*, *available at* 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).

[47] 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.

French cases about search "autocompletion,"[48] as well as numerous instances of French courts issuing extraterritorial orders.[49] 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,[50] including orders to affirmatively monitor and filter online content, including on third-party sites,[51] which runs counter to safe harbors in the E-Commerce Directive.[52] 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.

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

---

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*.

[48] Paris Court of Appeal, Dec. 9 2009, *Google Inc v. Direct Energie*, *available 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*, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2985. In 2011, the Paris Court of Appeal found that it was possible for Google to avoid obvious infringements of personality, and thereby reasonable to impose such an affirmative obligation. *See* Paris Court of Appeal, Dec. 14, 2011, *Lyonnaise de Garantie v. Google France, Google Inc, Eric S.*, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3303 (*aff'g* Paris Tribunal de Grande Instance, May 18, 2011, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3169).

[49] *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, *available at* 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, *available at* http://online.wsj.com/article/SB10001424052702304743704577382204111836554.html.

[50] Karin Matussek, *Google Loses German Copyright Cases Over Image-Search Previews*, Bloomberg, Oct. 13, 2008, *available at* 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, *at* http://cyberlaw.stanford.edu/blog/2013/12/german-supreme-court-finds-ebay-liable-actively-promoted-third-party-copyright.

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

[52] 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, *available at* http://www.businessweek.com/news/2012-04-20/google-s-youtube-must-help-detect-illegal-uploads-court-says.

over third party content,[53] 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.[54] Courts in Italy are also prone to deny safe harbor protection on dubious bases.[55]

Online platforms have even been subject to criminal complaints,[56] 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."[57] Although the conviction was ultimately overturned, for nearly three years the executives faced the prospect of criminal prosecution for third-party content.[58] 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,[59] 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

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

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

[55] *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.

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

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

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

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

establishing sufficient safeguards to prevent misuse and abuse of the takedown process.[60] A study by Copenhagen Economics[61] 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. 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,"[62] and executives faced possible prison terms, in addition to financial penalties,[63] based on legal standards that are essentially strict liability.[64]

Pakistan

YouTube has been blocked in Pakistan since September 2012, joining Facebook and Twitter, which were already blocked. Last year, Pakistan's new minister for IT and telecommunications 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]

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."[66]

Vietnam

---

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

[61] Copenhagen Economics, *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Global Network Initiative, March 2014, *available at* https://globalnetworkinitiative.org//sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

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

[63] 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.

[64] 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.

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

[66] 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.

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."[67]

V. 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.

Furthermore, as numerous studies have pointed out,[68] Internet platforms and services empower small- and medium-sized businesses to participate in international trade like never 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.

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

[68] *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, *available at* http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2012/10/25/000158349_20121025161729/Rendered/PDF/wps6253.pdf; McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity*, *supra* note 10.