Before the
Office of the United States Trade Representative
Washington, D.C.

In re	
Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers	Docket No. 2016-0007

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
REGARDING FOREIGN TRADE BARRIERS TO U.S. EXPORTS
FOR 2017 REPORTING

Pursuant to the request for comments issued by the Office of the United States Trade Representative (USTR) and published in the Federal Register at 81 Fed. Reg. 46,994 (July 19, 2016), the Computer & Communications Industry Association (CCIA) submits the following comments for consideration as USTR composes its annual National Trade Estimate Report on Foreign Trade Barriers (NTE).

I. INTRODUCTION

CCIA represents technology products and services providers of all sizes, 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]

The Internet is now a central component of cross-border trade in both goods and services. The removal of barriers to Internet-enabled international commerce is thus increasingly critical to U.S. economic interests. Given U.S. leadership in high-tech innovation and Internet technology, removing obstacles 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

[1] A list of CCIA members is available at https://www.ccianet.org/members.

that it has made significant contributions to U.S. output, employment, consumer welfare, trade, innovation, productivity, and corporate financial performance."[2]

International markets continue to present the most significant growth opportunities for major 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] Today, only six of those leading brands are U.S.-based,[4] vying for some 3.4 billion Internet users across the world.[5] Most recently, China overtook the United States as the largest market in the world for App Store revenue, earning 15% more than the United States over the third quarter of 2016.[6] CCIA thanks USTR for highlighting digital trade as a key priority in the 2016 NTE, and encourages USTR to continue this pursuit in years to come.[7]

U.S. trade policies and priorities have not sufficiently adapted to reflect the increasing importance of Internet-enabled trade to the U.S. economy. While trade policy has dramatically reduced barriers to trade in goods, the United States is increasingly becoming a services economy, with service industries employing a large majority of U.S. private-sector workers.[8] Meanwhile, the United States is the largest global exporter of services, exporting $688 billion in

---

[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.

[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 52% 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, Alphabet, *Alphabet Announces Fourth Quarter and Fiscal Year 2015 Results*, Feb. 1, 2016, https://abc.xyz/investor/news/earnings/2015/Q4_google_earnings/index.html. Similarly, 84.5% 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/ (last accessed Oct. 18, 2016) *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] Mary Meeker, *Internet Trends 2016*, June 1, 2016, at 187, http://www.kpcb.com/blog/2016-internet-trends-report.

[5] Internet Live Stats, http://www.internetlivestats.com/internet-users/ (last accessed Oct. 18, 2016).

[6] Sarah Perez, *China overtakes the U.S. in App Store revenue*, TechCrunch, Oct. 20, 2016, https://techcrunch.com/2016/10/20/china-overtakes-the-u-s-in-ios-app-store-revenue/ (referencing Lexi Snow, *Q3 2016 Index: China Hits an iOS App Store Milestone*, App Annie, Oct. 20, 2016, https://www.appannie.com/insights/market-data/q3-2016-index-china-hits-ios-app-store-milestone/).

[7] Office of the United States Trade Representative, *Fact Sheet: Barriers to Digital Trade*, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade (last modified Mar. 2016) (hereinafter "*Fact Sheet: Barriers to Digital Trade*").

[8] 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 Feb. 5, 2016).

2014 (a growth of 4 percent over the previous year.)[9] 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.

These developments call for maintaining and expanding the NTE's focus on digital trade barriers. To that end, these comments identify key obstacles to digital trade, including infrastructure 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. PROMINENT DIGITAL TRADE-RELATED BARRIERS

CCIA's comments are structured by country, but the following section contains a general survey of major issues that U.S. Internet and technology firms are facing abroad.

A. Data and Infrastructure Localization Mandates

As CCIA has noted in previous NTE filings, a number of countries are pursuing data localization policies, including mandated server localization and data storage.[10] Citing domestic privacy protections, defense against foreign espionage, law enforcement needs, and the promotion of local economic development, governments are considering these policies at an increasing rate.

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.[11] 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

---

[9] World Trade Organization, *International Trade Statistics 2015* (2015), at 46, https://www.wto.org/english/res_e/statis_e/its2015_e/its2015_e.pdf.

[10] Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information* (Sept. 2015), at 6, http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.

[11] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 718-19 (2015), http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

emphasize decentralization over single points of failure.[12] Data localization measures also distract from the development of global efforts to counter criminal activity online, while undermining the international cooperation that is necessary to promote cross-border law enforcement access.

Even as tools of protectionism, data localization policies are likely to hinder economic development, rather than promote domestic industry.[13] Such policies invariably restrict domestic economic activity[14] and impede global competitiveness.[15]

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.[16]

B. 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, with one recent study finding that countries lose

---

[12] 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.

[13] *See* Leviathan Security Group, *Quantifying the Costs of Forced Localization* (2015), http://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf (finding that "local companies would be required to pay 30-60% more for their computing needs than if they could go outside their country's borders).

[14] 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.

[15] 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.

[16] *See* Chander & Lê, *Data Nationalism*, *supra* note 11; 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*").

$23.6 million (per 10 million in population) for every day that the Internet is shut down.[17] Notwithstanding these costs, governments continue to filter and block Internet content, platforms, and services for various reasons. For example, as discussed further below, the services of many U.S. Internet platforms are either blocked or severely restricted in the world's largest market: China. In its 2015 report, Freedom House assessed that global Internet freedom had declined for the fifth consecutive year due to growing online censorship and monitoring practices.[18] It also reported that since 2014, 32 of the 65 countries assessed in the report have been on a negative trajectory,[19] with increases in political censorship, prosecutions for speech, and surveillance. 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. A recent Brookings Institution estimate pegged the global loss of intermittent blackouts at no less than $2.4 billion in one year.[20] Such blocking is likely to violate international commitments, such as the World Trade Organization's rules on market access and national treatment.

Methods of filtering and blocking generally consist of (a) legal or regulatory obligations imposed upon intermediary services, (b) network-level blocking and/or filtering achieved through state control of or influence over communications infrastructure, or (c) technology mandates that either hobble user privacy and security, or that force product manufacturers to include intrusive monitoring technology. 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,

[17] Deloitte, *The economic impact of disruptions to Internet connectivity, A report for Facebook* (Oct. 2016), http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf.

[18] Sanja Kelly, *et al*., *Freedom on the Net 2015: Privatizing Censorship, Ending Privacy*, Freedom House (2015), https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf (hereinafter "*Freedom House 2015*").

[19] *Id.* at 2.

[20] Darrell M. West, *Global economy loses billions from internet shutdowns*, Oct. 6, 2016, Brookings Institution, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf (hereinafter "Darrell M. West, *Internet shutdowns*").

Uzbekistan, and Vietnam.[21] 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.[22]

A similar barrier to cross-border data flows is gateway filtering. When countries operate national firewalls, all foreign websites and services must pass through "gateways." Domestic Internet content, however, does not pass through the gateways to reach its own domestic market. This has the effect of systemically affecting the speed and quality of service of foreign websites and services vis-à-vis domestic Internet content.[23]

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.

C. Legal Liability for Online Intermediaries

Foreign countries have frequently imposed substantial penalties on U.S. Internet companies for conduct of third parties — something that is not permitted under U.S. law and that impedes the ability of U.S. online services to be a platform for trade.[24] These penalties impede U.S. Internet companies from expanding services abroad. This hurts not only Internet companies, but also denies local small and medium-sized enterprises Internet-enabled access to the global marketplace, similarly discouraging investment in and growth of domestic startups.[25] While U.S. Internet businesses have thrived domestically under carefully crafted legal frameworks, international asymmetries in liability rules frequently favor domestic plaintiffs.[26]

---

[21] *Id*.

[22] *Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 16, at 98.

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

[24] *See generally* Ali Sternburg & Matt Schruers, CCIA, *Modernizing Liability Rules to Promote Internet Trade* (2013), http://cdn.ccianet.org/wp-content/uploads/2013/09/CCIA-Liability-Rules-Paper.pdf.

[25] 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.

[26] 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*,

D. Imbalanced Copyright and *Sui Generis* Context/Link Taxes

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. 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 the 2016 NTE described (discussed *infra* pp. 19-21), 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. Service 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 "snippet tax." It is also at times formally described as "ancillary copyright" in that it is allegedly an "ancillary" IP right — yet it is in fact inconsistent with international IP law, violates international trade obligations, and constitutes a TRIPS-violating barrier to trade.

While only the European Union is seriously contemplating ancillary/neighboring rights protection at the moment, other jurisdictions have at times considered such proposals. This issue is discussed in greater detail below, in the European Union section.

E. "Backdoor" Access to Secure Technologies

Providers of digital devices and services have for many years sought to improve the security of their platforms through the deployment of technologies that safeguard the communications and commercial transactions that they enable. Recently, strong encryption has been increasingly enabled on now-ubiquitous smartphones and deployed end-to-end on consumer-grade communications services and browsers. Encrypted devices and connections

---

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).

protect users' sensitive personal and financial information from bad actors who might attempt exploit that information.[27]

Many countries, at the behest of their respective national security and law enforcement authorities, are considering or have implemented laws that mandate access to encrypted communications. Often the relevant provisions are not explicit, but mandate facilitated access, technical assistance, or compliance with otherwise infeasible judicial orders. Countries considering anti-encryption laws include the United Kingdom, France, Germany, Brazil, India, and China.[28] Russia has already imposed this requirement on companies operating in its jurisdiction through its "Yarovaya" laws.[29]

Such exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[30] Companies already operating in countries that have or are considering anti-encryption laws will be required to alter global platforms or design region-specific devices, or face fines and shutdowns for noncompliance. Companies that might have otherwise expanded to these markets will likely find the anti-encryption requirements to be barriers to entry. These concerns are recognized in the Trans-Pacific Partnership, which prevents countries from compelling manufacturers or suppliers to use a particular cryptographic algorithm or to provide access to a technology, private key, algorithm specification, or other cryptographic design details.[31]

F. Undue Restrictions on "Over-the-Top" Services

Several countries have proposed or implemented undue or unreasonable regulatory restrictions on so-called "over-the-top" (OTT) services. USTR should encourage these and other

---

[27] Bijan Madhani, *Blast from the Past: Learning Lessons from Previous Panics Over Ubiquitous Strong Encryption*, Disruptive Competition Project, Sept. 10, 2015, http://www.project-disco.org/privacy/091015-blast-from-the-past-learning-lessons-from-previous-panics-over-ubiquitous-strong-encryption/.

[28] Kevin Collier, *The Countries That Are Considering Banning Encryption*, Vocativ, Apr. 11, 2016, http://www.vocativ.com/307667/encryption-law-europe-asia/.

[29] Alec Luhn, *Russia passes 'Big Brother' anti-terror laws*, The Guardian, June 26, 2016, https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws.

[30] Harold Abelson, *et al.*, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, MIT Computer Science and Artificial Intelligence Laboratory Technical Report, July 6, 2015, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[31] Office of the United States Trade Representative, The Trans-Pacific Partnership: Promoting Digital Trade, Annex 8-B, https://ustr.gov/tpp/#promoting-digital-trade.

countries that may be considering similar regulations to promote policies to encourage greater growth and competition in ICT services. Maintaining a clear regulatory distinction between information services and telecommunication services has been critical to the development of Internet services and applications in the U.S. and elsewhere. Online services help drive growth in some of the most profitable services offered by telecommunications providers.[32] In addition, online 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.

III. COUNTRY-SPECIFIC CONSIDERATIONS

What follows is a non-exhaustive list highlighting a few examples of potentially trade-restrictive localization policies or policy proposals:

A. Brazil

Over time, Brazilian policymakers have implemented policies which prevented innovation and technological progress. These policies place many restrictions on international trade, including, for example: (a) through government procurement preferences and preferable margins for local information and communication technology goods and equipment,[33] (b) Brazil's Presidential Decree 8135, which requires federal agencies to procure e-mail, file sharing, teleconferencing and VoIP services from Brazilian federal public entities,[34] or (c) the CERTICS Decree implemented to check whether software programs are the result of Brazilian innovation.[35] Brazil is also home to various local content requirements, filtering obligations, and tax incentives for locally-sourced ICT goods. These policies have prevented innovation and technological progress, and constitute unlawful barriers to trade. Urging Brazil to repeal these measures, in addition to addressing the issues outlined below, will help increase international

[32] *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").

[33] *Government Procurement Law and Policy: Brazil*, Library of Congress, https://www.loc.gov/law/help/govt-procurement-law/brazil.php.

[34] Jeferson Ribeiro, *Bill would allow Brazil to decree local Internet data storage*, Reuters, Nov. 5, 2013, http://www.reuters.com/article/net-us-brazil-internet-idUSBRE9A30SI20131105.

[35] *Certificate of Technology and Innovation in Brazil*, CERTICS, http://www.certics.cti.gov.br/?page_id=7&lang=en.

trade of information and communication technology goods and equipment, allowing more U.S. tech companies to do business in Brazil.

Filtering & Blocking

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.[36] This order was issued in relation to the Brazilian "Marco Civil," which, as stated by the Electronic Frontier Foundation, "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."[37] Fortunately, the decision was reversed by an appellate court, citing the disproportionate impact caused by shutting down the whole service over a local investigation.[38] WhatsApp was blocked for the third time in eight months this past July but the ban was once again overturned for the same reasons listed above.[39] Nevertheless, the most recent WhatsApp ban cost the Brazilian economy an estimated $39 million in just one day.[40] Because these interruptions impose corresponding costs on U.S. service exporters, 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.

De Minimis Threshold

Brazil's de minimis threshold for duty-free importation remains at USD $50, which is applicable only to consumer-to-consumer transactions, and does not apply to business-to-consumer or business-to-business transactions.[41] The differential treatment and low de minimis threshold for consumer-to-consumer transactions create barriers to international trade by increasing transaction costs for Brazilian businesses while limiting consumer choice and

[36] Jonathan Watts, *Judge lifts WhatsApp ban in Brazil after ruling block punished users unfairly*, Dec. 17, 2015, https://www.theguardian.com/world/2015/dec/17/brazil-whatsapp-ban-lifted-facebook.

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

[38] Watts, *Judge lifts WhatsApp ban in Brazil after ruling block punished users unfairly*, *supra* note 36.

[39] *Id*.

[40] Darrell M. West, *Internet shutdowns*, *supra* note 20, at 9.

[41] *Overview of de minimis value regimes open to express shipments world wide*, Global Express Association, Apr. 2016, http://www.global-express.org/assets/files/Customs%20Committee/de-minimis/GEA-overview-on-de-minimis_April-2016.pdf.

competition amongst Brazilian businesses. Extending the de minimis threshold to business-to-consumer and business-to-business transactions and raising the de minimis threshold would help Brazil conform with international consumer standards and shopping behaviors.

B. Canada

De Minimis Threshold

Canada has one of the world's lowest de minimis thresholds for goods coming across the border at $20 CAD — a threshold that has not been adjusted since the 1980s.[42] This low, de minimis level includes shipped goods, which has a huge effect on digital trade. Recent studies have shown that the small gains realized by collecting duties on these shipped goods is heavily outweighed by the costs of processing the large amount of shipments that fall below the de minimis level.[43] Encouraging Canada to raise the de minimis level on shipped goods and imports would result in a huge economic gain for both the U.S. and Canada by ensuring fairness for Canadian consumers, improving economic and government efficiency, and reducing the amount of hurdles small businesses operating internationally must jump over.

C. China

Data Localization

Chinese authorities have issued comprehensive guidelines for the treatment of personal data within information systems, requiring either (1) express consent of the data subject or (2) explicit regulatory or legal approval before personal data may be transferred abroad.[44] Chinese 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

---

[42] Andy Blatchford, *Feds Urged to Bump Up Duty-Free Limit For Canadian Shoppers*, The Huffington Post, Mar. 16, 2016, http://www.huffingtonpost.ca/2016/03/16/ottawa-faces-renewed-calls-to-let-canadians-spend-more-without-paying-duty_n_9481262.html.

[43] *See generally* Christine McDaniel, Simon Schropp, & Omin Latipov, *Rights of Passage: The Economic Effects of Raising the de minimis Threshold in Canada*, C.D. Howe Institute, June 23, 2016, https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/E-brief_Rights%20of%20Passage_June16.pdf (stating "we find that lifting the threshold would have a net economic benefit of up to C$648 million.").

[44] On July 16, 2013, China's Ministry of Industry and Information Technology (MIIT) promulgated the Provisions on Protecting the Personal Information of Telecommunication and Internet Users, which went into effect on September 1, 2013. Dianxin He Hulianwangyonghu Geren Xinxi Baohu Guiding (电信和互联网用户个人信息保护规定) [Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the Ministry of Indus. & Info. Tech. July 16, 2013, effective, Sept. 1, 2013) (Lawinfochina) (China), *available at* http://www.lawinfochina.com/display.aspx?id=14971.

national interests."[45] The Chinese government also practices strong protectionism in their information technology industries. As USTR noted in the 2016 NTE,[46] foreign companies operating in cloud computing are forced to enter into joint partnerships with Chinese firms if they wish to conduct business within China,[47] 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.[48] China, along with Taiwan, Turkey, and India, also implements local-presence requirements for processing of payment transactions.[49]

The American Chamber of Commerce in China surveyed existing and proposed Chinese data localization policies and found a number of anticompetitive laws.[50] Just this year, two more laws were passed: a "counter-terrorism" law that requires Internet and telecommunication companies to create methods for monitoring content for terror threats,[51] and an online publishing law that requires that all servers used for online publications and press are located within China.[52] In an interview with Reuters, President Obama said that the new "counter-terrorism" 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

[45] Law of the People's Republic of China on Guarding State Secrets, Art. 2, *available at* http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383925.htm.

[46] Fact Sheet: Barriers to Digital Trade, *supra* note 7 ("With regard to basic telecommunication services, China only permits foreign suppliers to enter into joint ventures with state-owned enterprises and imposes exceedingly high capital requirements").

[47] 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.

[48] U.S.-China Business Council, *Technology Security and IT in China: Benchmarking and Best Practices*, June, 2016, at 2, https://www.uschina.org/sites/default/files/Technology%20Security%20and%20IT%20in%20China%20-%20%20Benchmarking%20and%20Best%20Practices..pdf.

[49] *Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 16, at 86.

[50] 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. *See also* Comments of CCIA, *In re* Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers, Dkt. No. 2015-0014, filed Oct. 28, 2015, at 6-7.

[51] Bruce Einhorn, *A Cybersecurity Law in China Squeezes Foreign Tech Companies*, Bloomberg Businessweek, Jan. 21, 2016, http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies.

[52] David Barboza & Paul Mozurfeb, *New Chinese Rules on Foreign Firms' Online Content*, N.Y. Times, Feb. 19, 2016, http://www.nytimes.com/2016/02/20/business/media/new-chinese-rules-on-foreign-firms-online-content.html.

users of those services."[53]

A second draft of last year's cybersecurity law is also a cause for concern.[54] 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.[55] The law also requires that "the operators of key information infrastructures shall store within the territory of the People's Republic of China citizens' personal information and critical business data collected and generated during their operations within the territory of the People's Republic of China."[56] 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.[57] This draft law has led to concerns from foreign ICT equipment manufacturers about the burdens it will place on their ability to operate and introduce new products into the Chinese market.[58] In October 2016, Chinese President Xi Jinping presided over the fourth Politburo meeting dealing with IT and ICT issues, pushing for policies likely to reduce foreign technology companies involvement in the Chinese market.[59] CCIA asks USTR to discourage policies restricting foreign companies' ability to enter the Chinese technology sector, and to promote policies focused on allowing free and open competition within China's borders.

China recently suspended rules that would have forced banks to turn over proprietary source code and encryption keys to the China Banking Regulatory Commission (CBRC),[60] an

---

[53] 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.

[54] AmCham China, Cybersecurity Law of the People's Republic of China (Draft) (Second Draft), http://business-center.amchamchina.org/uploads/media/default/0001/05/b78e2db2b147c09b8430b6bd55f81bc8299ea50f.pdf.

[55] 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.

[56] *Cybersecurity Law of the People's Republic of China (Draft) (Second Draft)*; *see also* 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.

[57] 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/.

[58] Michael Martina, *Business groups petition China's premier on cyber rules*, Reuters, Aug. 11, 2016, http://www.reuters.com/article/us-cyber-china-business-idUSKCN10M1DN

[59] Li Rongde, *Xi pushes for Homegrown Network Technology to Improve National Cybersecurity*, Caixin Online, Oct. 10, 2016, http://english.caixin.com/2016-10-10/100995147.html.

[60] 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.

action which followed USTR addressing this issue in the 2016 NTE.[61] However, reports suggest that the CBRC has solicited opinions on a new version of the rules from western technology companies.[62]

Filtering & Blocking

As CCIA explained to the U.S.-China Economic and Security Review Commission in 2015, barriers to digital trade in China continue to present significant challenges to U.S. exporters.[63] USTR acknowledged these challenges in the 2016 NTE, highlighting the burdens of China's filtering of cross-border Internet traffic have imposed, and recognizing that outright blocking of websites has worsened.[64] High-profile examples of targeted blocking of whole services have included China's blocking of major U.S. services including Facebook, Picasa, Twitter, Tumblr, Google search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare.[65] Informal estimates suggest that this blocking has easily cost American firms billions of dollars as they are pushed out of the market.[66] 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,[67] 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.[68] 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

[61] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.

[62] Lim & Maher, *supra* note 56.

[63] *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, http://www.uscc.gov/sites/default/files/Schruers%20Testimony.pdf.

[64] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.

[65] *Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 16, at 98.

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

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

[68] 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.

early 2015.[69] Numerous scholars have argued that China's actions violate WTO rules mandating open access and equitable treatment between foreign and domestic firms.[70]

The second draft of the cybersecurity law mentioned in the previous section also has a provision that would authorize Chinese authorities to terminate Internet access during "public security" emergencies.[71]

China has also taken several steps to crack down on tools used to evade its broad Internet firewall. In January 2015, China made moves to upgrade its Internet firewall to make it harder for people to circumvent it by using VPNs.[72] Last year, the country cracked down on special software tools hosted on GitHub, a website popular with open source enthusiasts,[73] by launching distributed denial of service attacks against the site.

D. European Union

The European Commission is in the process of presenting a number of regulatory proposals, addressing subjects including copyright, telecommunications, audiovisual, and "ePrivacy." Common to all proposals is a focus on regulating principally U.S.-based "online platforms" such as search providers, social media, and online marketplaces. CCIA agrees with 2016 NTE's assessment that "these initiatives appear motivated, at least in part, by legacy businesses struggling to compete against the efficiencies provided by Internet-based commerce. This underscores the risk that even well-intentioned goals can, if implemented through heavy-handed regulation, or even just threat thereof, seriously undermine innovative business development and hurt the EU's own efforts to inject more dynamism into its markets."[74]

Data Localization

Within the European Union, both Germany and France have pursued localization policies that represent trade barriers. France has made significant investments in French cloud computing

---

[69] 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.

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

[71] Cybersecurity Law of the People's Republic of China (Draft) (Second Draft), Article 51.

[72] 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/.

[73] 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.

[74] 2016 NTE, at 178.

firms, to establish a local infrastructure for data storage and processing, known as "*le cloud souverain.*"[75] French territorial authorities ("collectivités territoriales") are now required to use only service providers established in France to store and process data in the cloud.

Germany has mirrored France's efforts regarding localization, along with calls for a European data network.[76] Deutsche Telekom, the partially state-owned, largest telecommunications provider in Germany, has proposed a "Schengen area routing" that 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 claims to route data only through domestic servers.[77] Although the idea of "Schengen area routing" has fallen out of favor as of late,[78] USTR should be watchful of similar ideas in the future.

In May 2015, Germany proposed 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.[79] 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[80] for a period of four weeks.[81] The German Bundestag approved the bill in October 2015.[82]

---

[75] Chander & Lê, *Data Nationalism*, *supra* note 11, at 690.

[76] 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.

[77] 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.

[78] Ian Traynor, *Is the Schengen dream of Europe without borders becoming a thing of the past?*, The Guardian, Jan. 5, 2016, https://www.theguardian.com/world/2016/jan/05/is-the-schengen-dream-of-europe-without-borders-becoming-a-thing-of-the-past.

[79] 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/.

[80] 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/.

[81] 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/.

[82] 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

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.[83] 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. 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.[84]

Intermediary Liability/Mandatory User Monitoring, Filtering, and Blocking

In September 2016, the European Commission submitted a copyright proposal to the European Parliament that proposes to eliminate protections that limit online services' liability for misconduct by those services' users, requires proactive screening by service providers, and creates a "neighboring" pseudo-copyright restriction. These proposals would upend nearly two decades of established law, threatening U.S. digital exports by eliminating long-standing legal protections for online services that are a cornerstone of Internet policy. This subsection discusses the intermediary liability ramifications of this proposal; the next discusses the "link tax."

The EC proposal disrupts settled law protecting intermediaries by removing established protections from U.S. Internet services in the 2000 EU E-Commerce Directive, and by imposing an unworkable filtering mandate on hosting providers that would require automated "notice-and-

---

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.

[83] Monika Kuschewsky, *Data Localization Requirements Through the Backdoor? Germany's "Federal Cloud", and New Criteria For the Use of Cloud Servicesby the German Federal Administration*, Inside Privacy, Sep. 15, 2015, https://www.insideprivacy.com/cloud-computing/germanys-criteria-for-federal-use-of-cloud-services/.

[84] 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.

staydown" for a wide variety of copyrighted works. The EC proposal would dramatically weaken these long-standing liability protections, and suggests that most modern service providers may be ineligible for its protections.[85]

Like U.S. law, EU law contains an explicit provision stating that online services have no obligation to surveil users, or monitor or filter online content.[86] Online services have invested heavily in developing international markets, including Europe, in reliance on these provisions. The EC copyright proposal now implies that online services must procure or develop and implement content recognition technology. The proposal to compel affirmative filtering of all Internet content, including audiovisual works, images, and text, based on that content's copyright status, is alarming, and profoundly misguided.

Moreover, the EC proposal provides no specifics for what filtering a hosting provider must implement, effectively empowering European rightsholders to dictate U.S. services' technology in potentially inconsistent ways across Europe.[87] In short, a provider will never know when it has done 'enough,' short of litigating in every EU member state. Until the CJEU eventually addresses the question, affected hosting providers can expect inconsistent rulings and injunctions from lower courts in different countries.

The proposal also appears to compel online services to enter into contracts with an indeterminate set of copyright holders, involving indeterminate subject matter, and withholds protection on *all* subject matter (not just copyright) for failure to do so. The vagueness of the language in the EU's copyright proposal, and the likelihood of inconsistent rulings in different countries, threatens to give the EU veto power over U.S. innovation. U.S. platforms, especially small businesses and startups, will be deterred from innovating and competing due to the ambiguity, harming U.S. companies and their consumers across the world. This would likely cause incalculable damage to U.S. economy — not just for existing companies, but for startups as well.

---

[85] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016)593, Recital 38 (suggesting that entities engaged in "optimizing the presentation of the uploaded works or subject matter or promoting them…" may now be ineligible for existing protection).

[86] *Compare* 17 U.S.C. § 512(m)(1) *with* Directive 2000/31/EC art. 15(1).

[87] *See* Proposal, *supra* note 85, at art. 11.

For example, surveys of venture capitalists show that 88% of investors are less likely to invest in user-generated content platforms in regions that have this kind of ambiguous legal framework for intermediaries.[88] If the EU proposal were to pass, there would likely be a corresponding increase in risk for U.S. platforms doing business in EU, resulting in significant economic consequences for the U.S. digital economy that depends on the EU market. Furthermore, there is likely to be a ripple effect on the rest of the world, given the EU's international influence. By effectively revoking long-established protections upon which U.S. services relied when entering European markets, the proposal would hold hostage U.S. companies' investments for the benefit of EU rightsholders, establishing an insurmountable market access barrier for many U.S. services and startups.

Brussels is not the sole risk to established norms on limiting intermediary liability. EU courts are increasingly hostile to this principle. For example, the June 2015 European Court on Human Rights decision against Estonia-based news portal Delfi, imposing liability for comments posted under news articles on its site, is another examples of a growing tendency to "shoot the messenger."[89] *Delfi* is difficult to reconcile with more modern approaches to intermediary liability, such as 47 U.S.C. § 230 and Europe's own E-Commerce Directive. 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 liability risks.

Ancillary Copyright/Link Tax

In the 2016 National Trade Estimate, USTR expressed concern about a "link tax" at a time when two EU member states, Germany and Spain, had implemented laws targeting U.S. online services and news aggregators, describing the tax as "arbitrary".[90] As CCIA has explained in proceedings, restrictions on the ability to quote (*inter alia*) news content violate Europe's international commitments. Unfortunately, there is now a European Union-wide

[88] Matthew LeMerle *et al*., *The Impact of Internet Regulation on Early Stage Investment* (Fifth Era 2014), at 20, http://static1.squarespace.com/static/5481bc79e4b01c4bf3ceed80/t/55200d9be4b0661088148c53/1428163995696/Fifth+Era+report+lr.pdf.

[89] Delfi AS v. Estonia, Eur. Ct. H.R. 64569/09 (2015).

[90] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.

proposal for a "neighboring right" that would be more expansive than these previous laws and would squarely violate international legal obligations.[91]

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." As TRIPS incorporates this Berne mandate, compliance is not optional for WTO Members. A neighboring right is another form of snippet restriction and would violate this TRIPS commitment.

The EC proposal advances a new *sui generis* entitlement, branded a "neighboring right", for publishers in news content they publish. The proposal is a more expansive, EU-wide version of previous German and Spanish efforts.

The proposal specifically contemplates a link tax, since the language of the proposal states that it excludes "acts of hyperlinking *which do not constitute communication to the public.*"[92] Acts of hyperlinking which *do* constitute communication to the public, therefore, would be subjected to varying taxes in dozens of EU member states. Given how broadly EU courts appear to interpret Europe's sweeping "communication to the public right"[93] (a right not found in the corresponding section of the U.S. Copyright Act),[94] the breadth of this tax is potentially sweeping, and at best, highly uncertain.

The new approach extends beyond a link tax, however. It also empowers a new class of plaintiffs with a 20-year, retroactive, entitlement to control (at least) digital reproduction and digitally making available to the public press publications, independent of journalists' underlying rights in the news content. Article 11 will restrict the ability of online platforms to include news links and the snippets necessary to explain those links. CCIA urges the U.S. Government to engage directly with European officials to address concerns about this potential market access barrier.

---

[91] *See* Proposal, *supra* note 85, at art. 13.

[92] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016)593, Recital 33.

[93] GS Media BV v Sanoma Media Netherlands BV (C-160/15).

[94] 17 U.S.C. § 106.

As described in greater detail in CCIA's 2015 NTE submission, Germany's 2014 ancillary copyright law (*Leistungsschutzrecht*) remains in effect, irrespective of EU-wide neighboring rights regulation. By extending copyright protection to small text excerpts in search results, this law violates international obligations that require free quotation.[95]

As discussed more fully in CCIA's 2015 Special 301 submission,[96] the Spanish partial reform of intellectual property laws instituted a similar "snippet tax" that violates Spain's international commitments by subjecting normal quotations to a form of levy. This too is independent of the neighboring rights/link tax proposal currently being considered in Brussels. 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.[97] 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.[98] 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. companies and distorts established copyright law, but it also violates the EU and Spain's treaty and WTO commitments.[99]

EU-U.S. Safe Harbor and EU-U.S. Privacy Shield

The 2015 decision 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 led to considerable regulatory uncertainty for companies with transatlantic operations. The Safe

[95] *See generally* Comments of CCIA, *In re* 2013 Special 301 Review, Dkt. No. USTR-2012-0022, filed Feb. 8, 2013.

[96] *See* Comments of CCIA, *In re* 2015 Special 301 Review, Dkt. No. USTR-2014-0025, filed Feb. 26, 2015.

[97] Antonia Molloy, *Google News to shut down in Spain*, USA Today, Dec. 11, 2014, http://www.usatoday.com/story/money/business/2014/12/11/google-news-spain-to-cease-operations/20234251/.

[98] 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.

[99] *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), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504596.

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. As USTR acknowledged in last year's NTE: "The CJEU ruling has created tremendous legal uncertainty for both U.S. and European businesses dependent on the framework."[100]

Fortunately, a renegotiated framework for transatlantic commercial data transfers, the EU-U.S. Privacy Shield, went into effect on August 1, 2016, after almost a year of uncertainty.[101] Like the Safe Harbor before it, the new framework allows companies to sign up with the U.S. Department of Commerce to verify that their privacy policies comply with the data protection standards of the Privacy Shield.[102] While the Privacy Shield represents an important step forward in protecting customer data, its usefulness may be threatened in the future by court challenges or modifications presented during the annual review process. Any significant challenges to the Privacy Shield may threaten the viability of EU-U.S. data transfers in the future. In fact, one such effort to annul the new framework has very recently been filed at the lower court of the CJEU.[103]

An alternative mechanism for ensuring that data transfers meet EU adequacy requirements, standard contractual clauses, is currently facing a legal challenge at the CJEU by parties that allege such clauses are inadequate on grounds similar to those used to invalidate the Safe Harbor. Standard contractual clauses were employed by many businesses in the period following the Safe Harbor's invalidation, and remain an important secondary compliance mechanism given the ongoing evaluation of the Privacy Shield by companies and European data protection authorities. If the Privacy Shield and alternative tools are again invalidated, there will be no mechanism through which companies can legally transfer the data of EU citizens across the Atlantic for commercial purposes.

Forcing international companies to keep all personal data in Europe is not feasible and

---

[100] Office of the United States Trade Representative, 2016 National Trade Estimate Report on Foreign Trade Barriers, 2016, https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

[101] International Trade Administration, EU-U.S. Privacy Shield Program Overview, https://www.privacyshield.gov/Program-Overview (last accessed Oct. 19, 2016).

[102] European Commission, EU-U.S. Privacy Shield fully operational from today, Aug. 1, 2016, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704.

[103] Julia Fioretti & Dustin Volz, *Privacy group launches legal challenge against EU-U.S. data pact: sources*, Reuters, Oct. 20, 2016, http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN12Q2JK.

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.[104]

General Data Protection Regulation and "Right to Be Forgotten"

The EU General Data Protection Regulation (GDPR) was adopted on April 27, 2016, and will go into effect on May 25, 2018. The GDPR is intended to unify data protection methods for individuals within the EU and confront issues resulting from the export of personal data outside of the EU.[105] However, latent ambiguities in the text of the GDPR mean that much of the impact the bill will have will be determined by how EU data protection authorities interpret the text.

The 2014 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."[106] In the two years 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."[107] In August 2015, the UK's data protection authority ordered the removal of links to "current news stories

---

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

[105] *See* Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), June 11, 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety.").

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

[107] 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.

about older reports which themselves were removed from search results under the 'right to be forgotten' ruling."[108]

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) 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. However, this case is currently on appeal to France's highest court.[109] If this appeal were to fail, French authorities would have the ability to constrain what non-French Internet users are able to access under EU legal standards, essentially giving France extraterritorial control to stop citizens of other countries from finding legally published information.[110] Such a ruling would send a signal to other governments that their laws should have extraterritorial impact as well, potentially triggering international conflicts of law, and creating significant market uncertainty for companies seeking to host user content and communications on a global basis.[111]

The GDPR also includes a "right to erasure" provision, which codifies the "right to be forgotten" and applies it to all data controllers. Under Article 17, controllers must erase personal data "without undue delay" if the data is no longer needed, the data subject objects to the processing, or the processing was unlawful.[112] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4% of a company's global operating costs.

Putting the onus on companies to respond to all requests in compliance with the "right to be forgotten" ruling and Article 17 of the GDPR is administratively burdensome. For example, popular U.S. services have fielded hundreds of thousands of requests since the policy went into

---

[108] *Id*.

[109] Alex Hern, *Google takes right to be forgotten battle to France's highest court*, The Guardian, May 19, 2016, https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court.

[110] 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.

[111] Samuel Gibbs, *French data regulator rejects Google's right-to-be-forgotten appeal*, The Guardian, Sept. 21, 2015, http://www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal; *see also* Daphne Keller, *The new, worse 'right to be forgotten'*, Politico, Jan. 27, 2016, http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/.

[112] Regulation (EU) 2016/679, General Data Protection Regulation, Apr. 27, 2016, *available at* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

effect.[113] Processing these requests requires considerable resources because each request must be examined individually. Small and medium-sized enterprises that also offer similar services but without similar resources to field these requests could find that the "right to be forgotten" and "right to erasure" pose a barrier to entry into the EU. USTR should monitor the outcome of these requirements for adherence with international commitments.

Undue Restrictions on Over-the-Top Services

In the European Union, there have been discussions about using regulations to "level the playing field"[114] and correct for supposed market advantages of OTT services, most recently in the European Commission's review of the Audiovisual Media Services Directive,[115] and potentially in the Digital Single Market proceeding as well.[116]

In May 2016, the European Commission published its proposal to reform Europe's audiovisual rules. This proposal introduces notably two amendments that undermine market access for U.S. companies. The first amendment is a mandatory requirement for video-on-demand providers to include in their catalogues a 20% share of European works (i.e. a 20% quotas of European content). Currently under the review of the European Parliament, this quota could reach 30%. This measure could either force U.S. companies to buy large volumes of inexpensive European content or to reduce the number of non-European works in their catalogues.

The second amendment allows European countries targeted by the services of a video-on-demand provider to impose levies on this provider to finance EU Member States' cultural funds. In practice, this amendment destroys the "country of origin principle" for video-on-demand providers, a cornerstone of the current European audiovisual rules and one of the main incentives for U.S. companies to invest in the EU's audiovisual market. Under the current rules, video-on-demand providers have to comply only with the rules from their country of establishment to operate across the EU. With these amendments, video-on-demand providers would have to

---

[113] *See, e.g.*, Alex Hern, *Google takes right to be forgotten battle to France's highest court*, *supra* note 109.

[114] Directive (EU) 2010/13, Audiovisual Media Services Directive, Mar. 10, 2010, *available at* https://ec.europa.eu/digital-single-market/en/audiovisual-media-services-directive-avmsd.

[115] *Id.*

[116] European Commission Press Release, *A Digital Single Market for Europe*, May 6, 2015, http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

contribute to the cultural funds of up to 28 Member States. This would fragment the Single Market and significantly hamper the activities of U.S. companies in the EU's audiovisual market.

This reform also includes provisions that undermine the intermediary liability regime applicable to video-sharing platforms, by stipulating that "in case of conflicts", audiovisual rules would prevail over the European safe harbor's provisions.

E. India

Data Localization

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.[117] Indian authorities have contemplated extending localization policies to non-government communications as well,[118] 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.[119]

Filtering & Blocking

The Indian government regularly shuts down mobile Internet services across regions in response to local unrest and protests, to prevent what it calls "anti-national activity."[120] Often

[117] Chander & Lê, *Data Nationalism*, *supra* note 11, at 694-97; *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/.

[118] 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.

[119] 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.

[120] Hasit Shah, *Where 'Digital India' Ends*, Future Tense, Sept. 7, 2016, http://www.slate.com/articles/technology/future_tense/2016/09/india_champion_of_web_access_cuts_off_mobile_internet_in_kashmir.html.

the shutdowns are in response to or in preparation for actions that may cause disturbances or violence, ranging from protests over jobs, and wrestling tournaments to name a few.[121] These shutdowns stand in stark contrast to India's recent efforts to expand the Internet across the country, and have led CCIA members including Facebook and Google to weigh in by developing Service Restriction Orders.[122] The Brookings research noted above estimates that Internet shutdowns cost India's GDP $968 million over the 70 days it has been shut down so far this year.[123]

Intermediary Liability

While India has enacted legislation to limit service provider liability,[124] an 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.[125] 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,"[126] and executives faced possible prison terms, in addition to financial penalties,[127] based on legal standards that are essentially strict liability.[128] CCIA applauds USTR's inclusion of this issue in its 2016 NTE, and hopes that USTR will continue to pursue this pressing issue. Although India's Supreme Court earlier clarified some sections of the 2000 IT Act, its existing provisions have still been harmful to intermediaries. In October 2015, an administrator of a WhatsApp group was arrested when someone in his group shared a video

[121] Deji Bryce Olukotun, *The Absurd Excuses Countries Give for Shutting Off Internet Access*, Future Tense, July 21, 2016, http://www.slate.com/blogs/future_tense/2016/07/21/excuses_officials_give_for_shutting_off_internet_access_include_wrestling.html.

[122] *Id.*

[123] Darrell M. West, *Internet shutdowns*, *supra* note 20, *at* 7.

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

[125] 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.

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

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

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

depicting violence toward a cow and the prime minister (notwithstanding the fact that group administrators in this application could not even delete members' posts in this app).[129] Imposing liability on an intermediary who cannot technologically respond to content is tantamount to a prohibition on use of the application.[130]

Undue Restrictions on Over-the-Top Services

India's Telecommunications Regulatory Authority and Department of Telecommunications have proposed introducing licensing and regulatory obligations targeted at OTT VoIP.[131]

F. Indonesia

Data Localization

As USTR noted in the 2016 NTE, since 2012, service providers providing a "public service" have been required to localize data servers within the country.[132] USTR has noted that these requirements "could prevent service suppliers from realizing economies of scale, discourage investment, and inhibit the cross-border data flows that are essential to electronic commerce."[133] 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.[134]

As also noted in the 2016 NTE, the Indonesian government requires that the equipment used for certain wireless broadband services contain certain levels of local content, and that telecommunication providers use half of their capital expenditures on network development of

[129] 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.

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

[131] *TRAI seeks to regulate OTT players like Skype, Viber, WhatsApp, and Google Talk*, The Indian Express, Apr. 18, 2015, http://indianexpress.com/article/technology/social/trai-seeks-to-regulate-ott-players-like-skype-viber-whatsapp-and-google-talk/.

[132] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.

[133] *Id*.

[134] Chander & Lê, *Data Nationalism*, *supra* note 11, at 698.

locally sourced components and services.[135] Additionally, Indonesia has issued a regulation that requires 4G enabled devices to contain 30% local content.[136]

Undue Restrictions on Over-the-Top Services

Indonesia's Ministry of Communications and Informatics released draft OTT regulations that essentially require offshore online services to come onshore or face a higher tax rate.[137] This law would require data localization, new liability and monitoring requirements for online services, creation of a local entity or permanent establishment, and numerous other market access barriers.

G. Iran

Filtering & Blocking

In May 2014, Iran blocked access to Google's hosting platform, Google Sites, and censored at least two Wikipedia pages.[138] The country also continues to block Twitter and Facebook, with YouTube being blocked intermittently, while some government officials have pushed to block WhatsApp and Viber.[139] Freedom House also ranked Iran as the worst country for Internet freedom in its 2014 report,[140] and Iran tied for second worst in 2015.[141] In late 2014, reports from Iran suggested that the country would impose a filtering system, rather than blocking websites outright. In February 2016, Iranian Communications and Information Technology Minister Ali Asghar Amidian announced that the Iranian government, in connection with several Iranian universities, spent $36 million to develop a "smart filtering" system intended to implement selective blocking of specific content.[142]

---

[135] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.

[136] *Id.*

[137] *MCIT issues draft regulation on OTT in Indonesia*, TeleGeography, May 5, 2016, https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/.

[138] 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/.

[139] 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.

[140] 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.

[141] *Freedom House 2015*, *supra* note 18.

[142] *Iran to Spend $36 Million on Internet "Smart Filtering," to No Avail*, International Campaign for Human Rights in Iran, Feb. 23, 2016, https://www.iranhumanrights.org/2016/02/iran-will-spend-36m-on-smart-filtering/.

H. Mexico

Mexico's Customs Agency seeks to drastically modify its simplified imports model by increasing the Value Added Tax and the duty for express shipments, transforming their simplified model into one more in line with the definite imports model.[143] The proposed changes would force higher prices, extended product shipment wait times, and decreased product selection on customers. Rejecting these proposed changes, and sticking with a simplified imports model will help fuel the growth of the tech industry in Mexico, will give consumers a wider selection of tech products at competitive prices. USTR should raise this issue in the upcoming NTE, and encourage the Mexican government to ensure compliance with its international trade commitments, such as the TPP, and evaluate the alternative rule proposed by courier companies.

In addition to sticking with a more simplified imports model, digital trade could flourish better if the large number of Mexican agencies that issue official regulation coordinated more to work within the NOMS requirements.

Mexico should also resolve ambiguities surrounding the types of data that can be stored in the cloud by reviewing upcoming cloud computing legislation. More transparency and accountability on both of these fronts would lead to increased growth of e-commerce in Mexico.

I. Nigeria

Data Localization

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

[143] On June 22, 2016, Mexico's Tax Administration Service issued a ruling announcing amendments to the current Foreign Trade Rule 3.7.3 and proposed new rule 3.7.35; *see (Mexico) SAT publishes new amendments to general foreign trade rules*, edicom, July 19, 2016, http://www.edicomgroup.com/en_US/news/8488-mexico-sat-publishes-new-amendments-to-general-foreign-trade-rules.

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, "[t]he goal is to promote development of domestic production of ICT products and services for the Nigerian and global markets, but the guidelines present 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."[144] One analysis concluded the guidelines "will prop up domestic technology enterprises at the expense of higher quality and/or more efficient foreign ones."[145]

J. Pakistan

Filtering & Blocking

Both Twitter and Facebook have intermittently been blocked in Pakistan, while Facebook is also routinely asked by the government to censor material deemed "blasphemous".[146] The popular blog site WordPress was also temporarily blocked for several days earlier in 2015 with little explanation from authorities.[147] These blocks have cost the Pakistani GDP an estimated $69 million dollars so far this year.[148]

K. Russia

Data Localization

As CCIA observed in its 2015 NTE submission, Russia signed localization measures into law in July of 2014,[149] which went into effect on September 1, 2015. The law requires all operators that process the personal data of Russian citizens to maintain databases located in

---

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

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

[146] *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/.

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

[148] Darrell M. West, *Internet shutdowns*, *supra* note 20, *at* 3.

[149] 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.

Russia, and to disclose the address of these databases to the Russian telecommunications authority.[150] In August 2015, the Ministry of Communications and Mass Media issued "clarifications" explaining the law's provisions, indicating that the localization requirements will apply to business activities that are "oriented towards" a Russian audience.[151] 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,[152] as well as the requirements to inform Russia's telecommunications authorities.[153] CCIA thanks USTR for emphasizing this issue in the 2016 NTE,[154] and hopes that USTR will continue to highlight this issue moving forward.

Roskomnadzor, the Russian agency responsible for enforcing the new data localization laws, conducted 302 inspections for compliance with the new law in 2015 alone, though Roskomnadzor Head Alexander Zharov reported the inspections revealed only minor infractions that he believed would be easily fixed, and would not lead to fines.[155] However, Zharov also stated that Roskomnadzor intends to evaluate at least 1,500 inspections in 2016 under the new law.[156] While initially Roskomnadzor indicated it would focus inspections on small to medium-sized companies, Roskomnadzor notified Facebook and Twitter of the various requirements of the law, and indicated both companies could be subject to audit in the future.[157]

---

[150] Reports have differed on whether regulators insist on data being *exclusively* located within Russia.

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

[152] 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

[153] 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/.

[154] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.

[155] Anthony L. Gallia, Luke P. McLoughlin, Maxim A. Voltchenko, *Russia's Personal Data Localization Law: Expanding Enforcement*, Lexology, Apr. 27, 2016, http:www.lexology.com/library/detail.aspx?g=b6eee37a-06b4-431a-9053-5400265739ed.

[156] Bret Cohen, Natalia Gulyaeva, Maria Sedykh, *Russia Data Localization Update: Results from Regulatory Inspections Clarify Enforcement Approach*, Hogan Lovells: Chronicle of Data Protection, June 23, 2016, http://www.hldataprotection.com/2016/06/articles/international-eu-privacy/russia-data-localization-update-results-from-regulatory-inspections-clarify-enforcement-approach/ (hereinafter "Cohen, Gulyaeva, and Sedykh").

[157] *See* Sergei Blagov, *Russia Pledges More Data Localization Audits*, Nov. 12, 2015, Bloomberg BNA, http://bna.com/russia-pledges-data-n57982063580/; *see also Interview with Alexander Zharov*, http://rkn.gov.ru/news/rsoc/news34448.htm (in Russian).

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 Russia's GDP). Further, investment would drop by -1.41% or 187 billion rubles.[158] These losses also reflect lost export opportunities for U.S. service providers. In the wake of the new law, 45,000 companies have informed Roskomnadzor that they comply with the law.[159]

Filtering & Blocking

Russia's 2012 Internet blacklist law, depending how expansively it is used, has the potential to block numerous American owned websites and services.[160] 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."[161]

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.[162] Russia also temporarily suspended Reddit in summer 2015 after a Russian user posted about psychedelic mushrooms. While the site was restored, Reddit now suppresses certain posts or subsections of its site for different countries, based on requests from authorities.[163]

"Right to Be Forgotten"

In addition to the EU and France, Russia adopted a "right to be forgotten" law, which took effect January 1, 2016.[164] The law requires search engine operators to delete personal information that is false, obsolete, or violates Russian law; however, search engines working on

---

[158] 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/.

[159] Cohen, Gulyaeva, and Sedykh, *supra* note 156.

[160] 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.

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

[162] 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.

[163] 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.

[164] *Russia's 'right to be forgotten' bill comes into effect*, RT, Jan. 1, 2016, https://www.rt.com/politics/327681-russia-internet-delete-personal/.

behalf of the government are excluded from the law. The law requires search engine operators to remove the infringing content within three to ten days, or the individual requesting deletion may go to court and get a warrant demanding removal of the information.[165]

L. South Korea

Extraterritorial Regulation

On September 23, 2016, South Korea's Amendment to the Act on the Promotion of IT Network Use and Information Protection became law. The Amendment provides for stricter penalties in the case of a data breach than were originally provided for in the Act, in addition to heavy fines for noncompliant overseas transfer of information.[166] U.S. tech firms have been threatened with investigations and fines for not complying with the more stringent regime, even though the data at issue is not subject to South Korea's physical jurisdiction. The extraterritorial enforcement of South Korean laws forces these firms to adjust the way they operate both in South Korea and globally.

M. Thailand

Intermediary Liability

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."[167] The 2007 Computer Crime Act, while slightly amended earlier last 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."[168]

---

[165] *Id.*

[166] Colleen Theresa Brown, Yuet Ming Tham, Samuel Yim, *South Korea Enacts Stricter Penalties for Data Protection Violations by Telecommunications and Online Service Providers*, Sidley Austin LLP Data Matters, Apr. 22, 2016, http://datamatters.sidley.com/south-korea-enacts-stricter-penalties-for-data-protection-violations-by-telecommunications-and-online-services-providers/.

[167] 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.

[168] 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.

N. Turkey

Filtering & Blocking

CCIA has previously noted barriers to social media such as Twitter and YouTube in Turkey,[169] 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.'"[170] The recent unrest in Syria, and subsequent attempted coup of Turkey's government, has led to further government censorship, with Turkish authorities recently censoring websites and Twitter accounts accused of spreading Kurdish propaganda, including journalism sites.[171]

In June 2016, Turkey passed a law featuring an "Internet kill switch", which allows Turkey's Information and Communication Technologies authority to "partially or entirely" suspend Internet access due to war or in matters related to national security, without seeking ministerial oversight first.[172] Use of this law may have already led to shutdowns of various social media sites in Turkey over the past few months.[173]

O. Vietnam

Forced Localization and Intermediary Burdens

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.[174] This law has been accompanied by numerous burdensome regulations for service providers, including local storage of user registration information and complete histories of posting activities on "general

---

[169] 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.

[170] 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.

[171] 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.

[172] *Social media blocked in Turkey*, Turkey Blocks, Aug. 25, 2016, https://turkeyblocks.org/2016/08/25/social-media-blocked-turkey/.

[173] *Id*.

[174] *Id.* at 23.

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.[175]

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,[176] these policies should be considered if and when Vietnam were to implement that agreement.

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."[177]

Vietnam's Decree No. 55 also contains provisions that 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."[178] 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."[179]

Undue Restrictions on Over-the-Top Services

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.

---

[175] *Id.* at 24.

[176] Office of the United States Trade Representative, *The Trans-Pacific Partnership: Promoting Digital Trade*, https://ustr.gov/tpp/#promoting-digital-trade.

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

[178] 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.

[179] *Id.* at 3.

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 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.

IV. CONCLUSION

As numerous studies have pointed out,[180] Internet platforms and services empower small and medium-sized businesses to participate in international trade like never before. 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.

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 proliferate. To push back against these barriers, U.S. trade policy and enforcement priorities must continue to reflect the large and growing importance of the Internet to the U.S. economy and U.S. trade performance. CCIA looks forward to USTR continuing its "special emphasis" on barriers to digital trade[181] in this year's NTE.

October 27, 2016

[180] *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* 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.

[181] *Fact Sheet: Barriers to Digital Trade*, *supra* note 7.