Before the
National Telecommunications and Information Administration
Washington, DC

In re International Internet Policy Priorities	Docket No. 180124068–8068–01

COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the notice of inquiry[1] issued by the National Telecommunications and Information Administration (NTIA), the Computer & Communications Industry Association (CCIA) submits the following comments on the subject of international Internet policy priorities for 2018 and beyond.

CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[2]

I. Introduction

CCIA commends NTIA for seeking input on the international Internet policy issues it should prioritize this year, and for paying particular attention to the venues in which it should seek to achieve its policy goals. NTIA's work on international digital policy is essential to ensuring that the Internet remains a vibrant place for free expression and commerce.

In particular, NTIA should prioritize the following: 1) protecting and promoting the free flow of information online, including by addressing jurisdictional challenges posed by the Internet; 2) safeguarding and supporting the multistakeholder approach to Internet governance; 3) fostering international coordination in digital privacy and security issues; and 4) furthering an international regulatory environment that encourages innovation in emerging technologies.

[1] 83 Fed. Reg. 27313 (June 12, 2018).
[2] A list of CCIA members is available at http://www.ccianet.org/members.

II. NTIA should seek to promote the free flow of information online.

CCIA welcomes NTIA's focus on the free flow of information online. The Internet, which relies on cross-border information flows, is an integral component of international trade in both services and goods. According to the U.S. International Trade Commission, digital trade added $517.10-$710 billion to U.S. GDP in 2011 alone, and global e-commerce is now valued at $28 trillion.[3] However, in recent years countries have begun pressing for laws and policies that challenge the free flow of information online, often through the extraterritorial application of domestic law, or under the guise of promoting domestic innovation, national security, and privacy protections. As the Internet grows increasingly important to free expression and commerce, it is essential that NTIA and the wider U.S. government work in every available international venue to promote policies that safeguard the cross-border delivery of Internet services and challenge those that would hinder their growth.

A. Challenges to the free flow of information online

1. Data and infrastructure localization mandates

Worldwide, a number of countries are pursuing data localization policies, including mandated server localization and data storage.[4] In a 2017 report, the International Trade Commission included estimates that such localization measures have doubled in the last six years.[5] Citing domestic privacy protections, defense against foreign espionage, law enforcement needs, and the promotion of local economic development, foreign governments are considering these policies at an increasing rate. While rarely the stated intention, in practice many of these policies effectively keep foreign competitors out of their markets.

---

[3] U.S. Int'l Trade Comm'n, *Digital Trade in the U.S. and Global Economies, Part 2*, at 1 (Aug. 2014), https://www.usitc.gov/publications/332/pub4485.pdf [hereinafter "*2014 Digital Trade in the U.S. and Global Economies, Part 2"*]; Office of the U.S. Trade Rep., *2018 Fact Sheet: Key Barriers to Digital Trade* (2018), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital.

[4] A recent study by the Information Technology & Innovation Foundation listed most of the world's formal data localization policies identifying over 30 countries that have enacted such policies as of April 2017. *See* Nigel Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?,* INFORMATION TECHNOLOGY & INNOVATION FOUNDATION at 20 (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf. *See also* Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information* at 6 (Sept. 2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20%20September%202015.pdf.

[5] U.S. Int'l Trade Comm'n, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, at 16 (Aug. 2017), https://www.usitc.gov/publications/332/pub4716.pdf [hereinafter "*2017 Global Digital Trade 1*"].

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.[6] Data localization rules often centralize information in hotbeds for digital criminal activity, including Indonesia, Brazil, Vietnam, and Russia, working against data security best practices that emphasize decentralization over single points of failure.[7] 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.[8] Rather than promote domestic industry, data localization policies are likely to hinder economic development,[9] restrict domestic economic activity,[10] and impede global competitiveness.[11]

Data localization policies may also be in violation of international obligations. 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

---

[6] 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.

[7] 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, at 54-59 (Dec. 2013), http://www.computer.org/csdl/mags/co/2013/12/mco2013120054-abs.html.

[8] Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, BERKMAN CTR. FOR INTERNET & SOC'Y, Research Publication No. 2016-3 (Feb. 16, 2016), https://ssrn.com/abstract=2733350.

[9] *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).

[10] 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.

[11] For example, foreign investment will likely decline. Given the high cost of constructing data centers, many companies will simply opt out of serving markets with onerous data localization requirements, especially small- and medium-sized businesses. In 2013, the average cost of data centers in Brazil and Chile were $60.3 million and $43 million, respectively. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, WALL ST. J. (Nov. 13, 2013), http://online.wsj.com/articles/SB10001424052702304868404579194290325348688. *See also* U.N. Conference on Trade and Development, *Data Protection Regulations and International Data Flows* at 3, (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ("[I]f data protection regulations go 'too far' they may have a negative impact on trade, innovation and competition."); *ITIF supra* note 4 at 6-7 ("At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries (which will not naturally be home to a data center). Such barriers also prevent companies from transferring data that's needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services.").

trade in services.[12] Data localization mandates almost invariably fail to meet this standard. In addition, these regulations are often vaguely construed, inadequately articulated and, therefore, nearly impossible to effectively implement.[13] Many countries are contemplating how current trade rules relate to the digital economy and nature of cross-border data flows.[14] NTIA should engage with the U.S. Trade Representative and U.S. trade partners to ensure that trade facilitates cross-border data flows and discourages unjustified localization mandates.

2. Filtering and Blocking

Perhaps the most apparent barriers to the free flow of information are the outright filtering and blocking of online content, with one recent study finding that countries lose $23.6 million (per 10 million in population) for every day that the Internet is shut down.[15] Despite these costs, governments continue to filter and block Internet content, platforms, and services for various reasons. For example, the services of many U.S. Internet platforms are either blocked or severely restricted in the world's largest online market: China.

In its 2017 report, Freedom House assessed that global Internet freedom declined for the sixth consecutive year due to growing online censorship and monitoring practices.[16] It also reported that since June 2016, 32 out of the 65 countries assessed in the report have been on a negative trajectory,[17] increasing political censorship, prosecutions for speech, and surveillance. The 2016 observed a key trend where governments are increasingly targeting messaging and voice communications apps, while others are cracking down on users expressing political views

[12] Article XIV - XIV *bis* of the General Agreement on Trade in Services provides these exceptions. General Agreement on Trade in Services Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).

[13] *See* Chander & Lê, *Data Nationalism*, *supra* note 6; *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 3.

[14] The WTO is current engaged on discussions regarding e-commerce and whether current commitments should be updated to reflect the needs of the digital economy. The EU is also considering adopting a position on language regarding the free flow of data in its free trade agreements. While an encouraging step, the current language risks *justifying* more data localization measures around the world rather than removing them. The proposed Article B recognizes protection of personal data and privacy as a fundamental right, allowing each party to maintain safeguards "it deems appropriate" (i.e. whatever the country itself sees as justified) for that purpose. *See* Proposed Language, Horizontal provisions for cross-border data flows and for personal data protection, available at https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf.

[15] DELOITTE, *The Economic Impact of Disruptions to Internet Connectivity, A Report for Facebook,* at 6 (Oct. 2016), http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf.

[16] FREEDOM HOUSE, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy* (2017), https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf [hereinafter "*Freedom House 2017"*].

[17] *Id*. at 4.

on social media.[18] 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, but 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.[19] 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.[20] Known offenders who use some or all of these practices include Afghanistan, Burma, China, Cuba, Egypt, Guatemala, Indonesia, Iran, Kazakhstan, North Korea, Pakistan, Saudi Arabia, Syria, Tunisia, Turkey, Turkmenistan, Uzbekistan, and Vietnam.[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.

---

[18] FREEDOM HOUSE, *Freedom on the Net 2016: Silencing the Messenger: Communications Apps under Pressure (2016), at 1, https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf [hereinafter "Freedom House 2016"]* ("Users in some countries were put behind bar for simply 'liking' offending material on Facebook, or for not denouncing critical messages sent to them by others. . .The number of countries where such arrests occur has increased by over 50 % since 2013").

[19] Darrell M. West, *Global Economy Loses Billions from Internet Shutdowns*, BROOKINGS INSTITUTION (Oct. 6, 2016), https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf [hereinafter Darrell M. West, *Internet Shutdowns*].

[20] WORLD ECONOMIC FORUM, *Internet Fragmentation: An Overview* (2016), http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [hereinafter *"Internet Fragmentation"*].

[21] Darrell M. West, *Internet Shutdowns*, *supra* note 31; *Freedom House 2016 supra* note 18.

[22] *2014 Digital Trade in the U.S. and Global Economies, Part 2*, *supra* note 3, at 98.

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. 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.

3. Legal liability for online intermediaries

Foreign countries have frequently imposed substantial penalties on U.S. Internet companies for conduct of third parties—something that generally is not permitted under U.S. law and that impedes the ability of U.S. online services to be a platform for digital commerce.[24] U.S. firms operating as online intermediaries face an increasingly hostile environment in a variety of international markets which impedes 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]

The European Union is considering a copyright proposal that would eliminate established protections from a broad range of intermediaries in the 2000 EU e-Commerce Directive.[27] This proposal imposes also an unworkable proactive filtering mandate on these intermediaries that

[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, *Modernizing Liability Rules to Promote Internet Trade*, CCIA (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*, 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).

[27] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM (2016)593 final (July 14, 2016).

would require automated "notice-and-stay-down" for a wide variety of copyrighted works.[28] This would be a significant departure from the longstanding approach under the EU's E-Commerce Directive that has provided Internet services operating in EU Member States regulatory certainty. The vagueness of these requirements under current proposed texts, and the likelihood of inconsistent rulings across Member States, empowers European rightsholders to dictate which U.S. innovations are successful. It is encouraging that Members of the European Parliament took heed of the warnings expressed by civil society and industry,[29] and recently voted to reject the content filtering proposal and other concerning proposals such as the creation of a neighboring right (see below).[30] However, negotiations on the copyright proposal continue. NTIA should closely follow these developments and raise concerns, when appropriate, if further discussions threaten U.S. digital exports to the EU.

4. Imbalanced copyright

Legislatures in Europe and EU Member States have proposed or implemented new publisher subsidies styled as so-called "neighboring rights"—related to copyright—that may be invoked against online news search and aggregation services and raise concerns from a trade perspective.[31] These laws deter investment in online services and are a violation of international obligations.[32]

The creation of ancillary rights also conflicts with the growing universal approach to balanced copyright laws that provide relevant limitations and exceptions. NTIA should advocate

[28] *See generally* Maud Sacquet, *EU Copyright Reform - Last Minute Countdown for EU Countries*, Disruptive Competition Project (May 18, 2018), http://www.project-disco.org/european-union/051818eu-copyright-reform-last-minute-countdown-for-eu-countries/#.W0T6aNhKhTZ.

[29] *See* Copyright 4 Creativity, https://saveyourinternet.eu/ (last visited July 10, 2018).

[30] Press Release, European Parliament, Parliament to Review Copyright Rules in September, available at http://www.europarl.europa.eu/news/en/press-room/20180628IPR06809/parliament-to-review-copyright-rules-in-september.

[31] The U.S. Trade Representative has also identified these laws as a trade barrier. *2018 Digital Trade Barriers Fact Sheet*, *supra* note 3, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital ("These measures impose financial and operational burdens on U.S. firms that help drive traffic to publishing sites."); Office of the U.S. Trade Rep., *2017 National Trade Estimate Report on Foreign Trade Barriers* at 162 (2017), https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf.

[32] The imposition of a snippet tax conflicts with U.S. law and violates long-standing international law that prohibits nations from restricting quotation. These regulations not only undermine market access for U.S. online services and depart from established copyright law; they also contravene World Trade Organization (WTO) commitments. By imposing a levy on quotations, these entitlements violate Berne Convention Article 10(1)'s mandate that "quotations from a work . . . lawfully made available to the public" "shall be" permissible. As TRIPS incorporates this Berne mandate, compliance with Article 10(1) is not optional for WTO Members; non-compliance is a TRIPS violation. Berne Convention for the Protection of Literary and Artistic Works, Sept. 28, 1979, art. 10(1), amended Oct. 2, 1979 (emphasis supplied).

for the balanced copyright rules, such as fair use, that have been critical to the growth of the U.S. technology and Internet economy. This innovation is jeopardized by weak or nonexistent limitations and exceptions in the copyright laws of foreign countries. A 2017 study illustrated how U.S. firms operating abroad in regimes with balanced copyright law reported high incomes and increased total sales, encouraging foreign investment.[33] A CCIA study showed that in 2014, fair use industries accounted for 16% of the U.S. economy, employed 1 in 8 workers, and contributed $2.8 trillion to GDP.[34] U.S. exports of goods and services related to fair use increased by 21% from $304 billion in 2010 to $368 billion in 2014 driven by increases in service-sector exports.[35] These economic benefits are lost when a country fails to uphold similar protections in their own copyright laws, impeding market access for U.S. companies looking to export, while also deterring local innovation.

5. Undue restrictions on "Rich Interaction Applications"

Several countries have proposed or implemented undue or unreasonable regulatory restrictions on rich interaction applications (RIAs)[36]—a term that refers to applications that facilitate "rich interaction" such as photo/video sharing, money transferring, in-app gaming, location sharing, translation, and chat among individuals, groups and enterprises.[37] However, a recent study has shown the vast economic and societal benefits from RIAs.[38] Global GDP has increased $5.6 trillion for every 10% increase in the usage of RIAs across 164 countries over 16 years (2000 to 2015).[39]

---

[33] Sean Flynn & Mike Palmedo, *The User Rights Database: Measuring the Impact of Copyright Balance*, PROGRAM ON INFORMATION JUSTICE & INTELLECTUAL PROPERTY (Oct. 30, 2017), http://infojustice.org/archives/38981.

[34] CCIA, *Fair Use in the U.S. Economy: Economic Contribution of Industries Relying on Fair Use* (2017), http://www.ccianet.org/wp-content/uploads/2017/06/Fair-Use-in-the-U.S.-Economy-2017.pdf, at 4.

[35] *Id*. at 6.

[36] *See NTA Bans 'Viber Out' Service in Nepal*, THE HIMALAYAN TIMES (Sept. 26, 2017), https://thehimalayantimes.com/business/nepal-telecommunications-authority-bans-viber-out-service-nepal; *En 15 días estará la ley sobre las aplicaciones*, EL PAIS (Feb. 24, 2016), http://www.elpais.com.uy/informacion/dias-estara-ley-aplicaciones.html; Saad Guerraoui, Morocco Banned Skype, Viber, WhatsApp and Facebook Messenger. It Didn't Go Down Well, MIDDLE EAST EYE (Mar. 9, 2016), http://www.middleeasteye.net/columns/boycotts-appeals-petitions-restore-blocked-voip-calls-morocco-1520817507; Letter from Hans W. Vriens, Secretariat - Asia Internet Coalition to Ministry of Information & Communications (Jan. 6, 2015), *available at* https://www.aicasia.org/wp-content/uploads/2015/01/AIC-comments-on-OTT-Circular-2015-01-06_EN.pdf.

[37] The term RIA is distinguished from the commonly used phrase "over-the-top" services. The term OTT originates in the telecommunications industry and broadly describes *any* application or service traveling across telecommunications infrastructure.

[38] Dr. René Arnold et al., *The Economic and Societal Value of Rich Interaction Applications (RIAs)*, WIK WISSENSCHAFTLICHES INSTITUT FÜR INFRASTRUKTUR UND KOMMUNIKATIONSDIENSTE GMBH (May 2017), *available at* http://www.wik.org/index.php?id=879&L=1 [hereinafter "*RIA Study*"].

[39] *Id.*

As it engages in multilateral fora, NTIA should encourage countries that may be considering imposing antiquated regulations on these emerging services to instead promote policies that encourage greater growth and competition in ICT services. For example, Kenya, in its draft national ICT policy, acknowledges the contribution of RIAs to the economy.[40] Instead of raising regulatory barriers, Kenya has attempted to promote RIAs and other Internet-enabled services and to encourage telecommunication operators to evolve their business models.

Maintaining a clear, regulatory distinction between information services and telecommunication services has been critical to the development of Internet services and applications in the United States and elsewhere. Governments should recognize that RIAs can offer societal benefits to them and their citizens by ensuring closer links, so governments can be more responsive to the needs of the citizenry. RIAs help governments respond to emergencies and public health crises more quickly and accurately; they can also improve enterprise and government efficiency through Smart Cities initiatives.

Online services help drive growth in some of the most profitable services offered by telecommunication providers.[41] Indeed, RIA use has a substantial, positive impact on telecommunication providers' businesses, giving them more opportunities to earn revenue and finance new infrastructure because RIAs drive demand for connectivity. As RIAs develop and become more popular, consumers will want to spend more time online and subscribe to telecommunication services—increasingly mobile services but also fixed broadband.[42] For example, video and music streaming services require more bandwidth and better connections, so heavy users of such services and RIAs "are more likely to have upgraded their mobile and fixed [Interest access services] subscriptions within the last two years."[43] In addition, online services also present cost-saving and product-enhancement opportunities for telecommunication providers, such as the opportunity to substitute fully featured VoIP for circuit-switched voice.

[40] *National Information & Communications Policy, 2016*, Ministry of Information & Communications Technology, para 18.5 p 44, http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf.

[41] *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").

[42] *RIA Study*, *supra* note 38, at 19.

[43] *Id*.

B. Resolving jurisdictional challenges to the free flow of information

1. Extraterritorial applications of domestic law

Many of the Internet's positive impacts on expression and commerce are a result of its borderless nature. Complications arise when governments attempt to apply domestic laws to Internet activities that occur outside their borders without considering the equities of stakeholders outside their jurisdictions. Oftentimes, the result is that freedom of expression and commercial activity online suffer.

One particularly salient example is the 2014 ruling by the Court of Justice for the European Union (CJEU) on the "right to be forgotten," which 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."[44] In interpreting this ruling, some European 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.[45] The case is currently on appeal to France's highest court,[46] which referred legal questions to the CJEU last year.[47] 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.[48] Such a ruling would send a signal to other governments that their laws should have extraterritorial impact as well, potentially

[44] 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.

[45] Google released a report recently illustrating how it fulfills its obligations under the "right to be forgotten." The report also shows how complex implementation can be for an Internet services provider. Google, *Three Years of the Right to be* Forgotten (2018), https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view.

[46] 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.

[47] Request for a preliminary ruling from the Conseil d'État (France), Case C-507/17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (2017), http://curia.europa.eu/juris/document/document.jsf?text=&docid=195494&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=369957.

[48] 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.

triggering international conflicts of law, and creating significant market uncertainty for companies seeking to host user content and communications on a global basis.[49]

A similar outcome could have resulted from a Canadian trade secrets ruling. In *Equustek Solutions v. Jack*, Google was compelled by the Supreme Court of British Columbia to remove—from all its domains worldwide—indexes and references to the website of Datalink, a competitor to Equustek that had been found to have violated Canadian trade secrets and consumer protection laws.[50] Following two unsuccessful Canadian appeals, Google successfully obtained permanent injunctive relief in the United States District Court in the Northern District of California, which held that the Canadian order could not be enforced in the United States because it undermined U.S. law and free speech on the Internet.[51]

2. Approaches to resolving conflicts of law

We encourage NTIA to continue to engage with multistakeholder venues that are considering the question of jurisdiction online, to ensure that the perspectives of users, industry, digital rights groups, and governments are all heard. One such project is the Internet & Jurisdiction Policy Network, which has convened experts from all these constituencies and produced a number of policy options for addressing questions about cross-border government requests to access data and moderate content online.[52]

In attempting to address the potential conflicts of law issues posed by extraterritorial application of domestic laws, some recent legislation and legislative proposals may provide a useful path forward. The U.S. recently enacted the "Clarifying Lawful Overseas Use of Data" (CLOUD) Act, which allows U.S. law enforcement to use existing legal process to require disclosure of data stored with providers subject to U.S. jurisdiction—unless the provider reasonably believes the customer or subscriber is not a U.S. person; *and* the disclosure would create a material risk that the provider would violate the laws of a qualifying foreign

[49] 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/.

[50] *Equustek Sols. v. Jack*, [2014] B.C.S.C. 1063, https://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc1063/2014bcsc1063.pdf.

[51] *Google v. Equustek Sols.*, No. 5:17-cv-04207-EJD, 2017 U.S. Dist. LEXIS 206818 (N.D. Cal. Dec. 14, 2017); *but see Google v. Equustek Sols.*, [2017] 1 S.C.R. 824, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do (earlier holding that the Canadian worldwide interlocutory injunction against Google should be upheld).

[52] Internet & Jurisdiction Policy Network, Publications, https://www.internetjurisdiction.net/publications.

government.[53] Courts may quash such an order if, among other things, the court performs a comity analysis that accounts for the interests of a qualifying foreign government in preventing a prohibited disclosure and the likelihood of penalties to a provider or any employees of a provider as a result of inconsistent legal requirements imposed on that provider.[54] The European Commission recently proposed legislation to address service provider production of e-evidence pursuant to member state investigations, which includes similar comity provisions.[55]

NTIA should encourage other governments to include international comity principles, which allow for the voluntary and reciprocal consideration of the laws of other nations, in the conception and application of domestic laws that have potential for extraterritorial impact on Internet services as one means to help address possible conflicts of law.

III. NTIA should safeguard and promote the multistakeholder approach to Internet governance.

The multistakeholder approach to Internet governance remains the model that best supports the continued growth and success of the Internet. NTIA's involvement with the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs), the Internet Governance Forum (IGF), and other multistakeholder bodies lends support to the inclusion of the variety of perspectives in the stakeholder community, embracing Internet users, industry, civil society, technical experts, and governments. The multistakeholder approach ensures that flexible, innovation-friendly policies are prioritized in a way that protects human rights and avoids the imposition of top-down government regulation that could infringe on both of these priorities.

A. The IANA Stewardship Transition should not be unwound.

Among NTIA's recent priorities in Internet governance has been the transition of the administration of the IANA functions for DNS management to the global Internet community housed at ICANN. CCIA's members were active participants in the multi-year process of

[53] *See* CLOUD Act § 103(a)(1); to be codified at 18 U.S.C. § 2713.
[54] *See* CLOUD Act § 103(b); to be codified at 18 U.S.C. § 2703(h)(3).
[55] *Commission Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, at 48-50, COM (2018) 225 final (Apr. 17, 2018), https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

preparing for and completing the transition and CCIA publicly advocated for the transition and argued its merits before Congress and the courts.[56]

CCIA's position is that the IANA Stewardship Transition should not be unwound. The transition was a successful example of the open, inclusive, transparent, and accountable process that can be achieved through the multistakeholder approach to Internet governance. Efforts to unwind the IANA transition at this point risk disrupting the security, stability and resiliency of the DNS system. The accountability mechanisms established as part of this transition remain viable, but need to be respected by ICANN. NTIA plays a key role in ensuring that ICANN remains committed to fulfilling the obligations it made during the IANA stewardship transition. Rather than considering unwinding the transition, which would only lead to discord in the Internet community and uncertainty and instability in the DNS system, NTIA should hold it up as an exemplar for continued multistakeholder participation in Internet governance.

B. NTIA involvement at ICANN

NTIA has and should continue to effectively represent the values and interests of the United States, its businesses, and its Internet users in engagement with ICANN. In particular, NTIA's participation in the Governmental Advisory Committee (GAC) is essential to safeguarding free expression, civil liberties, rule of law, and innovation on the Internet, at a time when other GAC members might prioritize different issues. NTIA's ability to highlight the need for the perspectives of the Internet stakeholder community and technical expertise in ICANN, as compared to the lack thereof in intergovernmental bodies, is also essential.

A specific endeavor NTIA should continue to prioritize is improving the security and privacy of the DNS. Following on NTIA's letter to the Chair of ICANN's Board in April,[57] CCIA supports NTIA's efforts to encourage ICANN to explore the opportunities for parties operating reverse proxy services, DNS resolvers, and third-party content delivery services to play a role in providing enhanced ecosystem security, beyond deploying DNSSEC to users.

[56] *See* Ed Black, Congress Makes Mountains Out of Digital Molehills in Latest Internet Skirmish, THE HUFFINGTON POST (Sept. 16, 2016), https://www.huffingtonpost.com/entry/57dc0a83e4b04fa361d998a3?timestamp=1474038885873; *see* Brief for Computer & Communications Indus. Ass'n. et al. as Amici Curiae Supporting Defendants, *Arizona v. Nat'l Telecomm. & Info. Admin.*, No. 3:16cv274 (S.D. Tex. Sept. 30, 2016).

[57] Letter from David J. Redl, Administrator, Nat'l Telecomm. & Info. Admin., to Cherine Chalaby, Chair, ICANN Board of Directors (Apr. 16 2018), https://www.ntia.doc.gov/files/ntia/publications/redl_to_icann_on_registrar_issues_april_2018_1.pdf.

With regard to WHOIS and the EU's General Data Protection Regulation (GDPR), NTIA should play a leading role to ensure that ICANN resolves disagreement with the recommendations raised in the GAC consensus advice from both its San Juan Communiqué and Panama Communique. The purpose would be to meet ICANN's stated goal of preserving access to registration data currently contained in the WHOIS framework to the greatest extent possible.

C. Multilateral organizations should play a supporting role in Internet governance.

As detailed above, CCIA's position is that the multistakeholder approach is the most inclusive, rights-protective, and innovation-friendly model for Internet governance. In contrast, multilateral organizations, in which governments are the primary drivers of policymaking, tend to lack comparable levels of technical expertise and diverse perspectives, though there is some variance within multilateral models.

At one end of the multilateral digital governance spectrum is the Organisation for Economic Co-operation and Development (OECD). The OECD, through its Committee on Digital Economy Policy (CDEP), encourages some stakeholder participation in its digital policy initiatives, provides for interventions by industry and civil society, and hosts stakeholder days in conjunction with Ministerials.

By comparison, the International Telecommunication Union (ITU) is a less participatory venue for Internet policymaking. CCIA recognizes the ITU's historic efforts to ensure access to information and communication technologies (ICTs) to underserved communities worldwide, as well as its expertise in international, technical standards development and spectrum coordination. However, the ITU does not provide regular opportunities for stakeholder participation. Governmental Member States have exclusive voting power at the ITU, and participation by non-governmental stakeholders is generally limited to Sector Members required to pay to participate in sectoral Study Groups.

In light of these deficiencies, NTIA should insist that multilateral organizations like the ITU adhere to a strictly and narrowly defined mandate. CCIA encourages NTIA to push back against proposals that would expand the ITU's remit and work programs beyond its core competencies.

To the extent multilateral organizations engage with Internet governance, NTIA should encourage them to provide meaningful avenues for stakeholder contributions and steer them

away from top-down regulatory approaches to innovative technologies, but rather focus on educating member states on the benefits of such emerging technologies.

IV. International coordination is essential for digital privacy and security.

The trans-national nature of the Internet, information flows, and technology development in the digital ecosystem demand a collaborative international approach to privacy and security. NTIA should promote industry-led approaches and voluntary, consensus-based standards, encourage the use of the best available secure technologies, and advocate for smart, non-discriminatory privacy rules that do not impede global commerce and data flows.

A. Strong encryption is fundamental to digital security and privacy.

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. 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 protect users' sensitive personal and financial information from bad actors who might attempt to exploit that information.[58]

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 they mandate facilitated access, technical assistance, or compliance with otherwise infeasible judicial orders.

These exceptional access regimes run contrary to the consensus assessments of security technologists because they are technically and economically infeasible to develop and implement.[59] 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. NTIA should raise these concerns in the inter-agency process and urge other governments not to

[58] 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/.

[59] 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.

compel manufacturers or suppliers to use a particular cryptographic algorithm or to provide access to a technology, private key, algorithm, or other cryptographic design details.[60]

B. NTIA should encourage collaboration with and among industry.

As the Departments of Commerce and Homeland Security noted in their report on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," governments can "constructively influence the development of more secure products by steps such as supporting open, voluntary, industry-driven standards . . . "[61] These sorts of industry-led standards development processes ensure security best practices that are flexible enough to promote technological innovation while delivering the most up-to-date protections.

NTIA should also encourage other governments to empower leading technology and cybersecurity companies to collaborate with each other. This may require changes to liability regimes or market incentives,[62] including in the U.S., but they can lead to ecosystem-wide benefits. For example, over forty global companies recently joined the Cyber Tech Accord, by which they publicly commit to "protect and empower civilians online and to improve the security, stability and resilience of cyberspace," regardless of nationality, geography or attack motivation.[63]

C. International policy development in privacy and data protection

As noted above, some countries have enacted data protection laws that effectively require localization of data for companies to successfully comply, without any evidence of improved privacy outcomes for users.[64] Given the adverse impacts of data localization on global commerce and the free flow of information, NTIA should pursue data protection arrangements that facilitate commercial data flows across borders and raise data protection standards for all participants. NTIA should also support evidence-based policymaking that takes into account the perspectives of business and civil society, in addition to governments.

---

[60] Bijan Madhani, *Digital Issues in NAFTA: Cross-Border Data Flows and Cybersecurity*, DISRUPTIVE COMPETITION PROJECT (June 15, 2017), http://www.project-disco.org/21st-century-trade/061517-digital-issues-in-nafta-cross-border-data-flows-and-cybersecurity/.

[61] Dep't of Commerce & Dep't of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecoystems Against Botnets and Other Automated, Distributed Threats* at 23 (2018), https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf [hereinafter "*Botnet Report*"].

[62] *Id. at* 24.

[63] *See* Cybersecurity Tech Accord, CYBER TECH ACCORD, https://cybertechaccord.org/accord/.

[64] *See supra* Part II.A.1.

NTIA should advocate for countries to participate in the development and implementation of APEC Privacy Framework and Cross-Border Privacy Rules (CBPR) system. which requires participating businesses to develop internal data transfer privacy rules consistent with the APEC Privacy Framework endorsed by APEC economies in 2004.[65] Demonstrating its interoperability not only among participating economies, but also with other regimes, APEC has worked with the EU to streamline the application process for participating companies to use complementary data transfer mechanisms to operate in both regions.[66]

V. NTIA should promote an international regulatory environment that encourages innovation in emerging technologies.

NTIA's Office of International Affairs has long been an advocate for policies that support digital entrepreneurs and innovators. Emerging technologies that it should pay particular attention to in the near future include artificial intelligence and the Internet of Things, as ongoing policy conversations can shape whether and to whom the benefits of these technologies inure.

A. Artificial intelligence (AI)

Discussions on the future of the workforce, among other developments, have increased government scrutiny on AI, automation, and algorithmic data analysis. We encourage NTIA, independently and as part of the inter-agency process, to ensure that the G20 Summit and the pending OECD study on "Artificial Intelligence in Society" endorse outcomes that enable growth and innovation on these technologies in an ethical manner. This can be done by proactively promoting the development of AI through coordinating and securing international investment in research and education, while also adopting frameworks that hinge on investing in human capital, skills, and worker flexibility. Industry and governments must work together to develop medium- and long-term solutions to empower all people and sectors to participate freely, feel safe, and take advantage of the benefits of technological innovation.

[65] The Framework does not impose treaty obligations on member nations. Rather, it sets an advisory minimum standard and represents a consensus across member economies. *See* Sidley Austin, APEC Overview, The Privacy, Data Protection and Cybersecurity L. Rev. 19 (2014) *available at* http://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurityla__/files/apec-overview/fileattachment/apec-overview.pdf.

[66] Angelique Carson, *EU and APEC Officials Agree To Streamline BCR/CBPR Application Process*, IAPP, May 26, 2015, *available at* https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-bcrcbpr-application-process/.

Separately, we urge NTIA to argue against any proposed Resolutions at the ITU Plenipotentiary meeting that would assert a role for the ITU with respect to AI regulation, standardization, or development.

B. The Internet of Things (IoT)

As the Internet of Things quickly becomes a commercial reality, it has begun to receive significant regulatory scrutiny, with a particular focus on security. Security is essential to ensuring user trust in IoT devices and services, which could yield worldwide economic benefits from $4 trillion to $11 trillion in the ten years from 2015 and 2025[67]—if the consumer and regulatory environment are favorable to both deployment and innovative ecosystem security practices.

NTIA should prioritize two international policy objectives with respect to the Internet of Things. First, as we highlighted in our comments in response to NTIA's 2016 RFC on fostering the advancement of the Internet of Things:

> "When consumers purchase a 'connected device,' they are getting both a good and a service—the physical device's connection often comes paired with a service operated remotely, often without a separate monthly service fee. True, the consumer may also see an application interface used to control or view data from a connected device, but that app is just an aspect of the services associated with that particular purchased 'thing.' It is important to ensure that the inherent duality found in IoT products is reflected in the context of any consumer-protective best practices going forward."[68]

This is the chief educational burden that policymakers, regulators, and cybersecurity professionals face with respect to the security of edge devices and small networks. As consumers more regularly recognize that the IoT products they purchase are both goods and connected software services—with embedded applications no different than traditional software—they will begin to expect those devices to be secure at purchase and updated regularly once deployed. In response to these marketplace expectations, manufacturers will be more likely to disclose their patching and update lifecycles, maintain their IoT software and services, and design more secure products in the first place.

---

[67] James Manyika et al., *Unlocking the potential of the Internet of Things*, MCKINSEY GLOBAL INSTITUTE (June 2015), http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[68] Comments of CCIA, Docket No. 160331306-6306-01, NTIA at 2 (2016), *available at* http://www.ccianet.org/wp-content/uploads/2016/06/CCIA-Comments-NTIA-IoT-RFC-FINAL.pdf.

Second, as emphasized in Commerce and DHS' Botnet Report, NTIA should encourage its interlocutors in international digital policymaking to incentivize IoT security best practices and services that can be deployed at the network and infrastructure level, which can improve ecosystem security even when device-level protections are lacking.[69]

C. OECD's Going Digital Project

The OECD's Going Digital Project is meant to "bring about stronger and more inclusive growth from the digital revolution, [through] a coherent and comprehensive policy approach."[70] The OECD's evidence-based approach to policy development incorporates the perspectives of business and civil society stakeholders into a multilateral process. NTIA should advocate for light-touch digital innovation-friendly policies across sectors to give policymakers "tools they need to help their economies and societies prosper in a world that is increasingly digital and data-driven."[71] CCIA applauds NTIA's engagement at the OECD on this matter and looks forward to its continued involvement.

The OECD plays a valuable role in shaping international policy and the Going Digital Project will have an impact on global discussions on regulation and policy interventions regarding the digital economy. The horizontal approach touches on a variety issues including, but not limited to, classification of online platforms, competition, privacy, digital taxation, and AI. Unfortunately, there are indications that reports under this project take a biased approach to Internet services and emerging technologies. NTIA should encourage the OECD to carefully consider how its various reports under the Going Digital Project will be used to influence regulators around the world, and any recommendations should result from strong evidence-based analysis.

D. Spectrum Coordination

NTIA has an important role in policy development at the ITU, particularly regarding spectrum. One of the ITU's primary mandates is in the coordination and allocation of spectrum. The ITU also develops technical standards to ensure the interoperability of international telecommunication networks. CCIA applauds Assistant Secretary Redl's proactive approach in

[69] *See Botnet Report*, *supra* note 61, at 12.
[70] Going Digital Project, OECD, http://www.oecd.org/going-digital/project/.
[71] *Id.*

developing the Administration's spectrum policy.[72] Assistant Secretary Redl has recognized the importance of the U.S. leading in the race to next generation ("5G"), as well as finding spectrum bands and promoting flexible or shared uses that can support new technologies and burgeoning demand, and CCIA encourages NTIA to share these perspectives with its counterparts in other governments and international venues.

VI. Conclusion

CCIA is encouraged by NTIA's interest in prioritizing its work in international Internet issues. Given the importance of the free flow of information online to the continued success of the Internet as a platform for free expression and commerce, it is essential that NTIA and the U.S. government address challenges posed by restrictive policy proposals in a range of international settings, while working to promote the principles that have historically enabled the growth of digital services. NTIA should also safeguard and promote the multistakeholder approach to Internet governance, foster international coordination in digital privacy and security issues, and promote an international regulatory environment that encourages innovation in emerging technologies.

July 16, 2018

Respectfully submitted,

Bijan Madhani
Senior Policy Counsel
Computer & Communications Industry Association
655 15th Street NW, Suite 410
Washington, D.C. 20005
(202) 783-0070

[72] Remarks of Assistant Secretary Redl at the NTIA Spectrum Policy Symposium (June 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-ntia-spectrum-policy-symposium, ("As leaders in spectrum policy across government and industry, we must use this finite resource effectively, so we can fully support our 21st century wireless needs. We need to plan for the future – so there will be enough spectrum available for 5G, unlicensed, and the next generation of satellite systems that hold so much potential.").