Computer & Communications Industry Association
Tech Advocacy Since 1972

50TH 1972 2022

STATEMENT FOR THE RECORD OF THE
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

U.S. Senate Finance Committee Subcommittee on International Trade, Customs, and Global Competitiveness
"Opportunities and Challenges for Trade Policy in the Digital Economy"

The Computer & Communications Industry Association (CCIA) submits the following Statement for the Record following the November 30, 2022 Senate Finance Subcommittee on International Trade, Customs, and Global Competitiveness Hearing. CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.

CCIA welcomes this opportunity to provide the following recommendations on the U.S. Trade Policy Agenda relating to the digital economy.

The U.S. should continue to negotiate binding commitments in free trade agreements that pertain to digital trade and cross-border delivery of Internet-enabled services. The Digital Trade chapters of the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement represent the gold standard of digital trade provisions, and any agreement pursued by the United States that includes digital trade priorities should reflect those provisions. The United States could also consider new digital trade disciplines and other high-quality digital agreements around the world, such as provisions related to artificial intelligence cooperation found in the Singapore-Australia Digital Economy Agreement. It is clear that our trading partners around the world recognize the importance of getting trade rules for the 21st century right, and it would be a missed opportunity for the United States to delay its engagement on the global stage in forging frameworks that enhance U.S. competitiveness and reflect our values.

At the same time, the United States should not fundamentally overhaul trade policy to undermine the benefits robust trade engagement confers to U.S. industry and consumers. While policymakers are encouraged to reassess approaches to international trade in light of new challenges and the changing global economy, it would be a step backwards to revise these commitments in future agreements that expand exceptions and/or overall weaken the effectiveness of such rules. The United States should

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

continue to pursue high standard agreements that facilitate global commerce, rather than adopting the approach of China in crafting multilateral agreements that have broad exceptions that render commitments meaningless like it is in the case of the Regional Comprehensive Economic Partnership (RCEP). It is important to note that any obligations undertaken are only with respect to partners the United States has chosen, and thus fears that strong rules incentivize trade with or investment in nations whose interests are inimical to ours are misplaced.

Finally, it is also worth noting that IPEF members with whom we already have FTAs—Singapore, Korea, Australia—already benefit, by virtue of MFN status, from some of the key enhancements negotiated in USMCA, that are absent in our existing bilateral FTAs. Thus, for example, these FTA partners currently enjoy the benefits of strong data flow and data localization rules (including for financial services) that the United States does not enjoy in their markets.[1]

DIGITAL TRADE RECOMMENDATIONS[2]

- ***Enable cross-border data flows in digital services.***

U.S. trade policy should further enable digital trade and the U.S. should be ambitious in its negotiations with respect to data flows and localization barriers. Cross-border data flows are critical to digital trade, and forced localization mandates make it difficult for U.S. exporters to expand into new markets. Analysis from the OECD has revealed an increasing level of restrictiveness for digitally-enabled services in part due to restrictions on cross-border movement of data.[3] Cross-border data flows are the lifeblood of global digital trade and by extension the array of industries that increasingly rely on the Internet to compete in the global marketplace. In the U.S., the productivity gains and efficiencies enabled by data flows have boosted the economy by hundreds of billions of dollars.

With an uptick in data-related barriers in recent years, trade discussions and clear rules are critical to ensure that any restrictions on the transfer, storage, and processing of data are targeted in a manner that

[1] If these countries were to take on similar binding commitments in an FTA with another country, we would equally enjoy rights in their market under MFN, but no country has replicated USMCA standards in full.

[2] These Recommendations reflect more extensive recommendations CCIA has filed with the Office of the U.S. Trade Representative and Department of Commerce in ongoing trade discussions such as IPEF, available at https://www.ccianet.org/2022/04/ccia-offers-recommendations-for-u-s-policymakers-on-indo-pacific-economic-framework/.

[3] OECD Services Trade Restrictiveness Index: Policy Trends up to 2020, available at https://issuu.com/oecd.publishing/docs/oecd-stri-policy-trends-up-to-2020?fr=sNmVlNzYxOTI3Mw.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

does not unreasonably limit legitimate cross-border trade. Policies that restrict data flows, either directly through explicit data and infrastructure localization requirements, or indirectly for national security or other purposes, negate the productivity gains and efficiencies enabled by Internet platforms and cloud computing while often simultaneously undermining digital security globally.

The U.S. should continue to pursue rules that prohibit governments from interfering with data flows or the exchange of information online, and prohibit regulations or standards that condition market access, procurement, or qualification for widely-used certifications based on nationality of ownership, location of corporate headquarters, or size of company.

Specifically, rules should prohibit governments from imposing data localization or local presence requirements on data controllers or processors, as well as linking market access and/or commercial benefits to investment in or use of local infrastructure. Often, such policies not only restrict foreign market access and investment, they become counter-productive as they hinder services providers' ability to diversify and backup data, instead centralizing it all in one or a handful of local data centers. These rules should also extend to financial services. To the extent possible, these prohibitions should apply to both explicit and indirect measures such as ill-fitting privacy and cybersecurity measures, industrial policy, and censorship disguised as national security protections to keep data in a particular country.

CCIA cautions strongly against introducing new exceptions to trade rules applicable to localization and cross-border data flows as a response to claims that trade rules constraint domestic regulatory from activating in the public interest. While requirements over how data is stored, processed, and transmitted may well evolve over time, the existing rules do not constrain such evolution. In the rare cases where localization can be justified, existing exceptions provide broad scope for addressing legitimate policy concerns.

- ***Foster trust in digital services and growth of new technologies.***

Trust is fundamental to the growth and cross-border delivery of these services. Without adequate privacy protections and security in digital communications, governments may continue to enact restrictions on cross-border services citing perceived risks. Privacy and consumer protections and trade rules should work in tandem to further the goals of initiatives promoting trustworthy data flows. To that end, trade agreements should encourage the development of national privacy legislation that sets clear rules on the use of personal data domestically, promote the adoption of bilateral and multilateral

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

agreements on government access to data such as those being pursued by the OECD,[4] and commit to codify protections for valid basis for transfer of personal data such as the APEC Cross-Border Privacy Rules into domestic law.

With respect to artificial intelligence (AI), trade agreements should encourage the adoption and deployment of trustworthy AI technologies by referencing principles and agreements that reflect multi-stakeholder input such the OECD Council Recommendations on Principles for responsible stewardship of trustworthy AI or the goals referenced in the White House's AI Bill of Rights.

- ***Prohibit customs duties for electronic commerce.***

Imposing customs requirements on purely digital transactions creates significant and unnecessary compliance burdens on nearly all enterprises, including small and medium-sized enterprises (SMEs). The moratorium on imposing customs duties for electronic transmissions has been key to the development of global digital trade and shows the international consensus with respect to the digital economy. The moratorium was most recently renewed at the 12th WTO Ministerial Conference in June 2022, and the commitment not to impose duties on electronic transmissions is reflected in the number of commitments made in free trade agreements among multiple leading digital economies. Permanent bans on the imposition of customs duties on electronic transmissions are a frequent item in trade agreements around the world and have been part of all U.S. FTAs for the past two decades.

The United States should continue to embed in trade agreements commitments resulting in a permanent ban on the imposition of customs duties on electronic transmissions. Enshrining the moratorium in agreements would enhance bilateral trade while also continuing to discourage other countries from including electronic transmission in their domestic tariff codes, as one IPEC member, Indonesia, has already sought to do.

[4] *See* https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm; https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

- ***Prohibit unilateral and discriminatory taxes.***

International trade requires a consistent and predictable international tax system, and tax measures play a significant role in the global competitiveness of U.S. companies. Any country that the United States seeks a trade agreement with should not impose digital taxation measures that are discriminatory in nature and contravene long-standing principles of international taxation, and the U.S. should seek to include commitments not to pursue unilateral and discriminatory digital taxation measures in forthcoming trade and economic pacts.

- ***Address state-censorship practices and combat rising digital authoritarianism.***

Censorship and denial of market access for foreign Internet services has long been the case in restrictive markets like China, but it is becoming increasingly common in emerging digital markets, including those of major trading partners, and even in some larger developed markets and is accomplished through different tools and methods.[5]

Allied governments have a critical role to play in partnering with technology companies and leading in the defense of Internet freedom and open digital trade principles. Government-imposed restrictions of digital services and online content can take multiple forms, and the risks associated with each method or regulatory framework providing for censorship methods can vary greatly.

The U.S. should work with trading partners to address rising digital authoritarianism and state-censorship practices that pose threats to the open Internet and freedom of expression around the world. Countries should affirm commitments under Article 19 of the International Covenant on Civil and Political Rights as they apply to defending free expression online. Making Article 19 binding and enforceable under a trade agreement would significantly enhance the value of this commitment. Parties should pursue commitments to refrain from blocking or restricting access to lawful online content, digital services, and infrastructure underlying Internet delivery. This is consistent with the goals of the U.S.-led Declaration for the Future of the Internet that encourages like-minded countries to promote fundamental freedoms online and combat actions by authoritarian governments. The United States should look to embed similar commitments to ensure an open Internet in trade disciplines as well.

[5] The U.S. International Trade Commission released its report on foreign censorship policies in January 2022 and detailed how extensive these practices have become. U.S. INT'L TRADE COMM'N, Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businesses (Feb. 2022), available at https://www.usitc.gov/publications/332/pub5244.pdf at 21.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

- ***Secure digital communications and devices and prevent bans on encryption.***

Providers of digital devices and services continue 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.

Many countries, at the behest of their respective national security and law enforcement authorities, have passed 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. Other versions require access to or transfer of source code related to encryption as a condition of allowing technology imports. Such exceptional access regimes run contrary to the consensus assessments of security technologists because these rules are technically and economically infeasible to develop and implement. Companies already operating in countries that have or are considering anti-encryption or source code access 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 or facilitated access requirements to be barriers to entry.

The United States should continue efforts to promote regulatory cooperation and international standards and best practices for securing products and services. Trade agreements should contain commitments to promote encrypted devices and connections, and adherence to frameworks such as the NIST-developed Cybersecurity Framework. Specifically, the agreement should prevent 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. Similarly, the agreement should prohibit governments from conditioning market access, with appropriate exceptions, on their ability to demand access to cryptographic keys or source code.

Additionally, the agreement should include commitments for partners to pursue risk-based cybersecurity measures, and utilization of open, consensus-based international standards as they are the more effective approach in comparison to prescriptive regulation. Trading partners should pursue cooperative

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

approaches to cybersecurity and incident responses, including sharing of information and best practices with respect to vulnerability disclosure.

- ***Foster innovation in artificial intelligence.***

Emerging technologies such as artificial intelligence (AI) and machine learning, as well as quantum computing, increasingly impact cross-border trade, and trade rules increasingly govern the development and growth of these technologies. The United States should ensure regulatory practices and technical standards are in alignment to foster open lines of cooperation. To continue to use and export AI and other emerging technologies, businesses and users need a trade framework that allows them to move data and infrastructure safely across borders while ensuring that other countries will not misuse legal systems to impede the growth of new technologies. This will enable use of emerging technologies in addressing global challenges such as public health, humanitarian assistance, and disaster response. Work on promoting AI alignment and export competitiveness should not clash or otherwise undermine existing efforts such as the ongoing National Institute of Standards and Technology AI Risk Management Framework process aimed at implementing a risk-based and flexible AI regulatory landscape.

Trade rules that can facilitate the responsible cross-border growth of AI technologies include those that enable cross-border data flows and remove localization requirements; encourage governmental investment in and release of open data; identify and share best practices for the responsible use of AI; engage in cooperation and public-private collaboration on AI; and adopt innovation-oriented copyright rules that enable machine analysis of data. In addition, to ensure substantive convergence and avoid the potential for discriminatory outcomes, the U.S. and its trading partners should agree to avoid adopting any measures that discriminate against U.S. suppliers who excel in this area by providing less favorable treatment to AI products or applications than they give to like products or applications without an AI component.

As a matter of good regulatory practice, the development and implementation of AI regulations should include: adopting a risk-based approach, including transparent processes for assessing, managing, and mitigating risks associated with specific AI applications; assessing whether potential risks can be mitigated or addressed using existing instruments and regulatory frameworks; considering whether any new or proposed regulation is proportionate in balancing potential harms with economic and social benefits; employing risk management best practices, including considering the risk-substitution impact

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

of a specific AI application against a scenario where that application has not been deployed but baseline risks remain in place; and promoting the development of voluntary consensus standards to manage risks associated with AI applications in a manner that is adaptable to the demands of dynamic and evolving technologies.

In addition to trade rules, countries should work together to facilitate research and development of new applications of AI to address shared challenges; facilitate dialogues among all stakeholders including governments, civil society, academia, and the private sector on best regulatory practices; and pursue joint discussions on the responsible and ethical use of AI.

- ***Promote global practices on Internet access and interconnection policies.***

The United States should work to protect the interoperable and interconnected nature of the global Internet architecture that enables cross-border data flows, support principles of non-discrimination and market access to telecommunications networks, and enable stakeholders to negotiate the nature of services to be delivered across the network on a voluntary market-driven basis, based on reasonable business practices agreed upon by both sides.

Globally, the business practice on Internet interconnection is for content and application providers and ISPs to enter into agreements through autonomous negotiations. To protect the Internet ecosystem, the growth of the tech industry globally, and ensure these investments can continue to flourish and support digital trade, the United States should seek to include assurances that Internet-based telecommunications service providers seeking the exchange of traffic with content and application providers, and vice versa, are able to negotiate with the other party on a voluntary, market-driven basis in this agreement. Trade rules should prevent new mandates to negotiate with ISPs, and the unilateral imposition of fees, as a condition for reaching end-user customers. This builds on existing trade rules that ensure that access to domestic telecommunications networks is facilitated on reasonable and non-discriminatory terms.

- ***Commit to following good regulatory practices.***

The global Internet economy is at a pivotal moment in its development. Countries are moving quickly to introduce new, at times experimental, regulatory frameworks for digital services, and seek to craft rules on the development of emerging technologies with the aim to ensure that the digital economy remains a tool for openness and free exchange that has led to unprecedented growth and opportunity.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

As new proposals are introduced around the world, countries should commit to following good regulatory practice and work together to ensure that regulations do not have unintended impacts. International regulatory cooperation is an important tool for improving regulatory quality, reducing the likelihood of creating trade barriers or unnecessary regulatory differences, aligning regulation with shared principles and values, avoiding unintended consequences or conflicts with broader foreign policy objectives, building trust and expertise among regulators, and deepening understanding of trends in regulatory governance to inform current and future approaches to policymaking. As new regulations take effect in foreign markets, it will be essential that the U.S. work with trading partners to ensure that implementing regulations are fair, implemented in a non-discriminatory manner against foreign firms, and are subject to adequate oversight and due process.

The United States should pursue governing principles of the digital economy that ensure that regulations should be non-discriminatory and principles-based, made pursuant to a transparent regulatory process, ensure due process to those affected, and include adequate safeguards to reduce the impact of any unintended consequences.

- ***Address technical barriers to trade.***

U.S. technology exporters face a growing number of non-tariff measures such as technical regulations, conformity assessment practices, and standards-based measures. Adoption of global standards is critical to ensuring regulatory coherence and avoiding country-specific standards that deter market entry. Some U.S. cloud service providers (CSPs) have been unable to serve the public sector due to onerous security certification requirements that deviate from internationally accepted standards and make it impossible for CSPs to comply without creating a market-unique product, including physically segregating facilities for exclusive use for government-owned customers and onshoring of data. The adoption of country-specific standards creates de facto trade barriers for U.S. companies and raises the costs of cutting-edge technologies for consumers and enterprises.

The United States should (1) pursue commitments like those outlined in USMCA Chapter 11 on addressing technical barriers to trade; and (2) pursue commitments to follow good regulatory practices of these commitments in the development of standards, regulations, and conformity assessment procedures for services.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

- ***Enable trade in electronic payment services.***

Electronic payment (e-payment) systems which are interoperable across borders are critical in enabling the growth of cross-border digital trade. Trade policy can help drive the development of cross-border e-payment systems through commitments on the free flow of data including financial services data, promoting interoperability through international standards, and encouraging open innovation and competition through the adoption of open e-payment models such as real-time payments (RTP) systems and encouraging open application programming interfaces (APIs) to allow all e-payment service providers to compete. Additionally, the United States should pursue provisions on electronic signature, electronic authentication, paperless trading, and other best practices often included in trade agreements.

- ***Promote copyright frameworks that enable emerging technologies and digital services.***

As part of U.S. trade policy, the U.S. should promote intellectual property frameworks that reflect U.S. law and secure commitments that will foster innovation in emerging technologies. This is reflected in a few areas of copyright traditionally included in trade agreements.

First, a flexible copyright regime is necessary for the continued growth of the digital economy. Principles such as fair use are a cornerstone of U.S. copyright law and industries that rely on this right are a significant contributor to the U.S. economy and exports. Fair use is also critical to activities central to new areas of innovation and cutting-edge technology such as artificial intelligence and text and data mining. Additionally, mandated technological protection measures (TPMs) are a frequent inclusion in U.S. trade agreements. Corresponding statutory exceptions to these anticircumvention measures are a critical component of these provisions. Consistent with USMCA, any TPM provision should include exceptions to anti-circumvention that are consistent with 17 U.S.C. § 1201, including § 1201(f) on reverse engineering and interoperability, in providing limitations and exceptions to TPMs.

Intermediary liability protections for Internet service providers, such as the framework in Section 512 of the Digital Millennium Copyright Act in the United States, have been critical to growing the U.S. digital economy by providing business certainty to U.S. investors and innovators. U.S. trade policy has long reflected domestic copyright principles by including necessary intermediary protections for online services in trade agreements dating back to 2003. USMCA continues this tradition, drawing directly upon Title 17 of the U.S. Code.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 - Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org