Internet Regimes and WTO E-Commerce Negotiations

January 28, 2020

Congressional Research Service
https://crsreports.congress.gov
R46198

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46198

January 28, 2020

Rachel F. Fefer
Analyst in International Trade and Finance

Internet Regimes and WTO E-Commerce Negotiations

From retail to agriculture or healthcare, digitization has affected all sectors and allowed more industries to engage with customers and partners around the globe. Many U.S. companies thrived in the initial online environment, which lacked clear rules and guidelines, quickly expanding their offerings and entering foreign markets. As the internet has evolved, however, governments have begun to impose national laws and regulations to pursue data protection, data security, privacy, and other policy objectives. The lack of global rules and norms for data and digital trade is leading to differences in these domestic internet regimes. Competing internet regimes and conflicting data governance rules increase trade barriers and limit investment flows and international commerce, restricting the ability of U.S. businesses and consumers to enter and compete in some markets. For example, foreign internet regimes may use national security regulations to block cross-border data flows, disrupting global supply chains and limiting the potential use of and gains from emerging technologies. The creation of national technology standards can also limit market access by foreign firms.

As the digital economy expands, the diversity in digital rules is poised to grow in complexity and create new trade restrictions. The resulting patchwork of technical standards and national systems creates challenges for international trade, and may signal an impending fracturing of the global internet. Without agreement on global norms or common trade rules, some analysts foresee a splitting of the internet into distinct nation-led "dataspheres" and virtual trading blocs.

The internet is global, governed by common technical protocols; it may also be regulated at the national level, although there is no international consensus on the proper role for governments. The lack of multilateral trade rules governing the digital economy has led to efforts to establish common global rules and norms. Over 75 countries, including the United States, are participating in World Trade Organization e-commerce negotiations, which aim to establish a global framework and obligations to enable nondiscriminatory digital trade. Proposals by the United States, the European Union (EU), and China illustrate the variation in member objectives, highlight potentially controversial issues, and raise questions about the likelihood of meaningful consensus.

In general, the United States adopts a market-driven approach that supports an open, interoperable, secure, and reliable internet that facilitates the free flow of online information and supports other policy objectives such as privacy and national security. The EU, while supporting the role of the market and free flow of information also emphasizes the need for data protection, internal regional integration, and "technological sovereignty," a recent and evolving concept in the EU.

In contrast to the U.S. and EU approaches, which both emphasize the open global internet, China pursues a state-led approach that maintains a firewall between the Chinese internet and the rest of the world. China's government strictly controls the flow of information on its networks and restricts the companies who can participate in its digital economy. Many aspects of internet service and content in China are prohibited to U.S. firms. China is exporting its system through its direct export of goods and services, including surveillance technologies, and is trying to influence international standards and norms to allow space for China's model of strict state controls. Other countries, such as India and Vietnam, are building their own internet regimes, borrowing from the Chinese, European, and U.S. approaches.

Congress has an interest in addressing growing protectionist policies and trade barriers, and in developing U.S. rules and standards for internet governance that promote digital trade and economic growth, balanced among other policy objectives. The divergence in national internet regimes and its impact on digital trade raises numerous complex issues of potential concern to Congress. These include whether to support initiating new bilateral trade negotiations specific to digital trade; how the United States can conclude a successful plurilateral WTO e-commerce negotiation that achieves greater reciprocity and market access for U.S. exporters and removes barriers to trade; how such an outcome can be balanced with other policy objectives; and whether federal engagement in and support for international standards-setting bodies is sufficient.

Contents

Figures

Contacts

Introduction

National internet regimes, as defined by individual countries' domestic policies and rules, are growing more divergent, a trend that has significant implications for international trade and the future growth of U.S. and global digital economies. The evolving digital economy increases productivity and drives growth in the overall economy, but may be threatened by differences in national rules and potential fracturing of the global internet. Congress has an interest in ensuring the U.S. digital economy thrives and shapes the global rules and norms for digital trade.

As internet technology expanded from its origins in the military and defense sector into the commercial arena in the 1990s, consumers and firms began to conduct transactions in an online environment that lacked clear rules and guidelines.[1] Some U.S. firms took advantage of the open global commons and thrived, quickly expanding their offerings and entering foreign markets. In many foreign markets, U.S.-based Google dominates search and e-mail, Facebook is the number one social network, and Amazon is the first stop for online shopping. However, in certain other markets, some of which are important for the United States, trade barriers limit or block those same websites.

While national rules-setting may focus on domestic priorities, policies that affect digitization in any one country's economy can have consequences beyond its borders. The internet is a global "network of networks," and the state of a country's digital economy can have global ramifications, such as affecting the security and efficacy of connected networks. Differences in the internet governance and data policies of the United States and some major trading partners, such as People's Republic of China (PRC or China) and the European Union (EU), are creating a growing set of trade barriers for U.S. firms seeking to do business abroad. Trade barriers include, for example, rules and regulations governing foreign investment, market and network access, e-commerce, and data collection and usage. The United States generally advocates a free and open internet, using standard-setting forums and other means of international cooperation to ensure non-discriminatory market access, advance common emerging technology standards, promote collaborative open-source architecture, and influence the internet regimes of trading partners balanced with other public policy objectives, including national security.

Trade agreement negotiations present an opportunity to remove trade barriers and establish common trade rules and disciplines to achieve U.S. negotiating objectives. Across the globe, U.S. and other bilateral and plurilateral agreements have created a plethora of overlapping and often inconsistent rules between various trading partners. The lack of multilateral rules on digital trade is a key focus of U.S. trade policy. Ongoing e-commerce negotiations at the World Trade Organization (WTO) provide a significant opportunity to establish enforceable multilateral rules that align with U.S. policy priorities and help bridge growing differences in national rules and trade treatments. However, such negotiations face inherent challenges, including possibly divergent, and even conflicting, positions.

Congress has a strong interest in the rise of the varying internet regimes and their current and potential impact on U.S. digital trade and the economy. Through legislation and oversight, Congress can directly and indirectly shape U.S. internet policy and official positions in trade negotiations and international standard-setting forums. Congress pro-actively established U.S. digital trade negotiating objectives for trade agreements and has supported provisions in free trade agreements (FTAs) to address the lack of multilateral digital trade rules and market opening commitments, most recently in the U.S.-Japan trade agreement and the U.S.-Mexico-Canada

[1] For more information on the founding of the internet, see https://www.darpa.mil/about-us/timeline/modern-internet.

Agreement (USMCA). Congress can also influence U.S. positions in the ongoing WTO negotiations.

This report will compare some aspects of various national internet regimes and then examine the ongoing WTO e-commerce negotiations and certain international forums that present an opportunity to establish global rules and technology standards and to minimize or prevent potential problems created by diverging systems.

Digital Trade and Digital Economy

While no single definition or measure of the digital economy exists, according to the Bureau of Economic Analysis, the "digital economy" accounted for 6.9% of U.S. GDP in 2017, including (1) information and communications technologies (ICT) sector and underlying infrastructure; (2) digital transactions or e-commerce; and (3) digital content or media.[2]

Defining Digital Trade

The U.S. International Trade Commission (ITC) defines digital trade as:

> the delivery of products and services over the Internet by firms in any industry sector, and of associated products such as smartphones and Internet-connected sensors. While it includes provision of e-commerce platforms and related services, it excludes the value of sales of physical goods ordered online, as well as physical goods that have a digital counterpart (such as books, movies, music, and software sold on CDs or DVDs).[3]

According to the ITC definition, laptop sales are included in digital trade as is the transmission of an email or online purchase, but the t-shirt a consumer may order online is not.

From agriculture and manufacturing to healthcare, the collection, exchange, and processing of data is transforming and increasing productivity across the economy. Data is traded as end products (e.g., music file, marketing tools), inputs for producing digital and physical goods and services (e.g., 3D printing file, Uber), or sources of information leading to further action (e.g., real-time supply chain analytics).[4] New data is created every day by individuals sending text messages, sharing photos, or searching online, by automated machine-to-machine transmissions in manufacturing, or by vehicles in connected transportation systems. According to one calculation, 2.5 quintillion bytes (or 2.5×10^{18}) of data are produced daily.[5] To put that number into context, 2.5 quintillion bytes of data would fill 10 million blu-ray discs, the height of which stacked would measure the height of four Eiffel Towers on top of one another.[6] At the other extreme, a single short text message could represent 21 bytes and a single high-definition movie could require 4 million bytes.

[2] U.S. Bureau of Economic Analysis, *Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts*, March 2018, https://www.bea.gov/research/papers/2018/defining-and-measuring-digital-economy. Note: BEA did not include partially digital items, such as sharing economy services, in its estimates.

[3] For more information on digital trade, please see CRS Report R44565, *Digital Trade and U.S. Trade Policy*, coordinated by Rachel F. Fefer.

[4] Joshua Meltzer, Brookings Institution, World Trade Review, Volume 18, Special Issue S1 (Digital Trade) April 2019, pp. S23-S48.

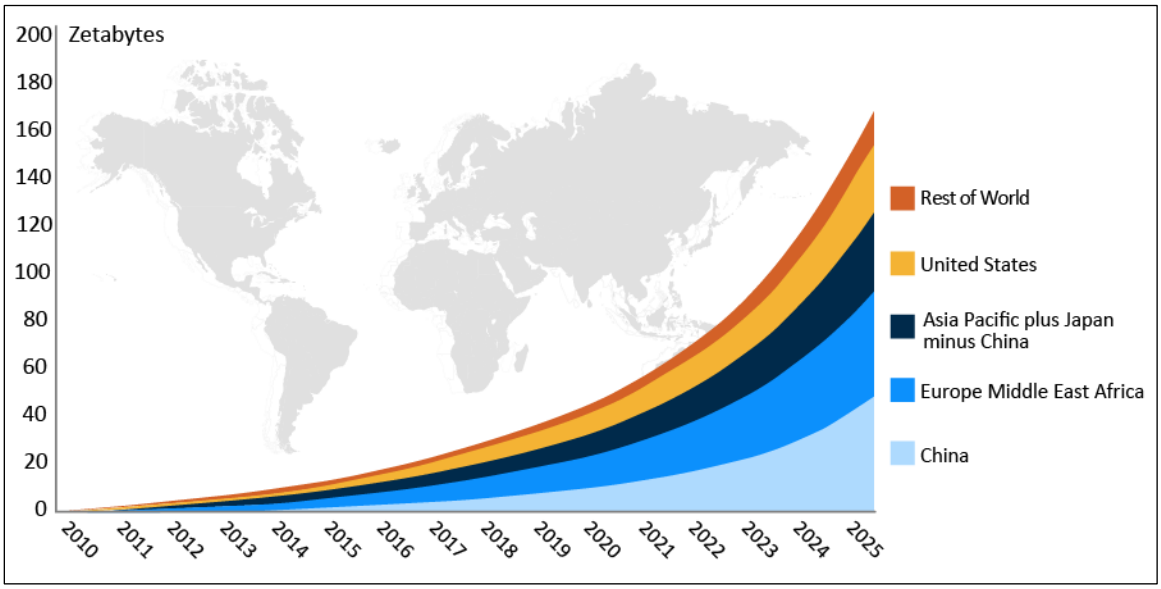
[5] William Schneider, Jr., "China, 5G, and Dominance of the Global 'Infosphere'," Hudson Institute, September 2019.

[6] http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/.

The digital economy depends on data flows to send data between individuals, organizations or devices, often crossing national boundaries. For example, in 2017, approximately 12% of international trade of physical goods was facilitated by e-commerce and almost 20% of China's imports and exports was enabled by digital platforms.[7] A separate study showed that digital products accounted for 70% of the U.S. services trade surplus in 2017.[8] Cross-border data flows grew by a factor of 45 between 2005 and 2016 and continue to expand.[9] The volume of global data flows is growing faster than global trade or financial flows, and its positive GDP contribution offsets the lower growth rates of trade and foreign direct investment (FDI).[10]

The global "datasphere" is expected to grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025.[11] One study predicts there will be more than 150 billion connected devices across the globe by 2025.[12] Today, China has the fastest-growing regional datasphere, while the U.S. datasphere is relatively mature, with an already high penetration of people online.[13] As China and other regions' dataspheres expand, the United States' and EU's relative shares of the global datasphere will decline (see **Figure 1**).

Figure 1. Global Datasphere by Region



Source: David Reinsel, et al. "The Digitization of the World From Edge to Core," IDC, November 2018, p. 17.

[7] Jacques Bughin and Susan Lund, "The ascendancy of international data flows," McKinsey Global Institute, January 9, 2017.

[8] Bertelsmann-Foundation, "The No Collar Economy," http://www.bfna.org/wp-content/uploads/2017/11/Bertelsmann-Foundation_The-No-Collar-Economy-LQ.pdf.

[9] Jacques Bughin and Susan Lund, McKinsey Global Institute, "The ascendancy of international data flows," *Vox*, January 9, 2017.

[10] Gary Clyde Hufbauer and Zhiyao Lu, Peterson Institute for International Economics, "Can Digital Flows Compensate for Lethargic Trade and Investment?" November 28, 2019.

[11] Datasphere refers to the notional environment in which digital data is stored. One zettabyte is equivalent to a trillion gigabytes. David Reinsel, et al. "The Digitization of the World From Edge to Core," IDC, November 2018, p. 16, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[12] Ibid.

[13] The report divides the global datasphere into China, United States, Europe-Middle East-Africa, and Asia Pacific-Japan-excluding China.

Note: 2018-2025 represents estimates.

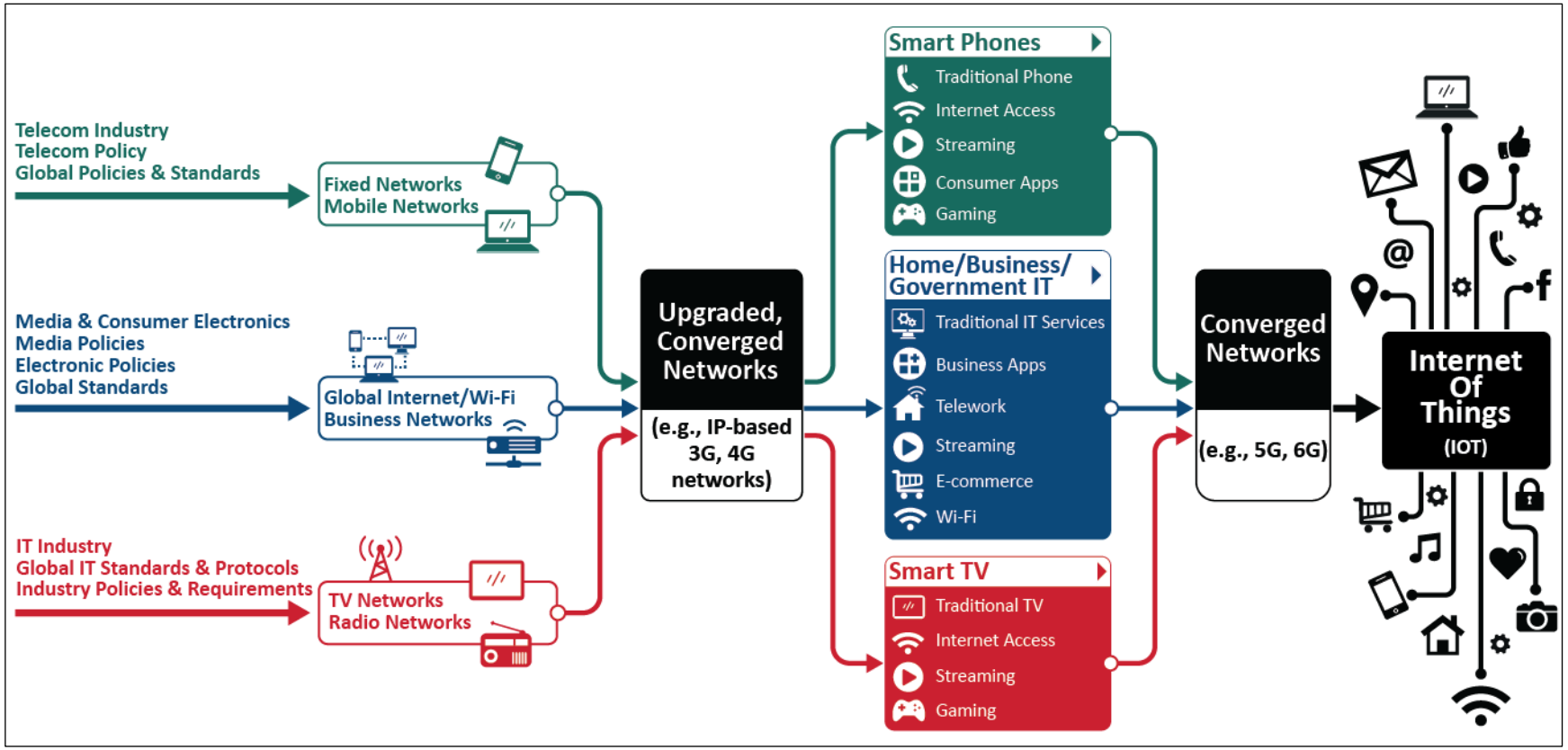
As the volume and importance of data grows, policymakers are increasingly interested in how data is gathered, stored, and used, and how to best balance policy goals and objectives, such as supporting international trade flows and protecting personal privacy. The future growth of the global digital economy and digital trade specifically will be shaped by the policies that govern global data flows and other internet-related rules set at national, regional, and multilateral levels. China's expected digital growth, in particular, may increase its ability to shape the rules of the global datasphere, which may not align with U.S. interests and could create additional trade barriers (see "The People's Republic of China (PRC)").

Technology Convergence and International Rules-Setting

The ICT sector is experiencing a convergence between technical spheres that had previously been separate and independent technologies: telecommunications, media and consumer electronics, and information technology (computers) (see **Figure 2**).[14] The ability to stream videos on multiple devices (e.g., television, tablets, mobile phones) demonstrates the convergence of technologies and previously separate services. Separate policies, technical standards and protocols traditionally governed each sub-sector, but today companies that provide services across all sectors and the governments that traditionally regulated these services separately must wrestle with how best to govern the converged spheres.

[14] CRS Report R45746, *Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues*, by Suzy E. Park.

Figure 2. ICT Convergence



Source: CRS.

Although there are common technical protocols governing the flow of traffic, interconnections, and data transfers across networks, there is no single set of international rules or disciplines that govern key digital trade issues such as electronic contracts or cross-border data flows, and the topic is treated inconsistently, if at all, in trade agreements. The lack of multilateral rules governing the digital economy has led, on the one hand, to countries creating diverging national policies and, on the other hand, to efforts to establish common global rules. Countries may seek common rules on some digital issues, such as technical standards, but set different national rules on others (e.g., privacy, data protection) to reflect domestic priorities or cultural norms. Governments may also try to shape international standards and norms to benefit their domestic industries.

The emergence of national internet regimes that govern and divide the global datasphere raises a number of issues. First, national regimes allow a government to create rules and policies that advance domestic priorities and reflect local norms. Without shared rules or interoperability between national regimes, differing requirements for internet and data governance can lead to increased trade and investment barriers, which can restrict the willingness and ability of businesses and consumers to enter some markets. U.S. firms offering services that can be traded remotely using the internet or another digital network (so-called "potential" ICT-enabled [PICTE] services) can be blocked from markets with discriminatory restrictions in place.[15] For example, many U.S. firms' inability to access the Chinese online market raises growing concerns about discrimination and protectionism, as other countries may emulate China and its internet regime.[16]

Second, the existence of globalized supply chains that dominate international trade may be threatened if rules governing national or regional dataspheres do not provide for reciprocity or limit companies' ability to share data with global subsidiaries, partners, or customers. Disrupted trade and global supply chains could not only result in limited growth of individual companies, but could also impede a country's economic competitiveness if participation is limited to those entities within what amounts to a virtual trading bloc. For example, Qualcomm might not be able to sell its chips to some countries if the technical requirements vary nationally, or John Deere might not be able to service customers in certain markets if data flows with its U.S. headquarters are blocked. Similarly, the diffusion of knowledge and potential gains from emerging technologies that depend on global economies of scale could be impeded by diverging standards or regulations that create artificial borders and constrain data aggregation thereby, for example, diminishing effective development of artificial intelligence and machine learning which depends on collecting and processing vast volumes of data.

Third, as in other areas of international trade, the party(ies) that ultimately set the global internet rules and technical standards for data and emerging technologies will gain first-mover advantage. Past industry experience suggests that companies who are the first to market new technologies often capture the bulk of the revenues. To that end, some governments have actively promoted their domestic policies in an effort to convince other countries to adopt similar regimes that may not align with U.S. policies and priorities. For example, China promotes its national standards and technologies through international sales of its domestic technologies based on domestic technical standards, particularly in Africa and Latin America. Furthermore, some countries in these regions have begun to import China's internet-sovereignty policies, a form of what some consider to be digital authoritarianism (see discussion below).

[15] PICTE services as defined by Department of Commerce Bureau of Economic Analysis (BEA).

[16] For example, many websites and apps are blocked in China, see: https://startuplivingchina.com/list-websites-apps-blocked-china/.

The EU also aims to set global standards on competition and privacy through its rules and enforcement actions that compel multinational technology firms to change behavior and adjust business models. For example, the EU actively promotes its data privacy regime by requiring that trading partners have "adequate" domestic data privacy regimes (as judged by EU authorities) to allow for the bilateral free flow of personal data that many companies depend on to operate. Individual EU countries may impose further requirements for security purposes that could further constrain a business's operations.

OECD Digital Services Trade Restrictiveness Index (DSTRI)

The DSTRI captures changes in countries' regulatory barriers limiting services trade digitally.[17] The DSTRI scores show that the U.S. system is relatively open compared to other markets and that China remains the most closed digital economy. Looking across all countries, the study found that overall digital trade restrictiveness increased between 2014 and 2018.

The DSTRI also scores restrictiveness across a number of sub-categories. For example, for electronic transactions, Brazil, China, India, and Indonesia score as the most restrictive countries on the index, while Russia has the same score as the United States and EU countries.[18] In contrast, for infrastructure and connectivity, Russia is the most trade restrictive (tied with Colombia and South Africa).[19] Russia's score reflects its new so-called internet sovereignty law that allows the country to potentially cut itself off from the global internet and aims to eliminate users' ability to bypass state web filters.[20]

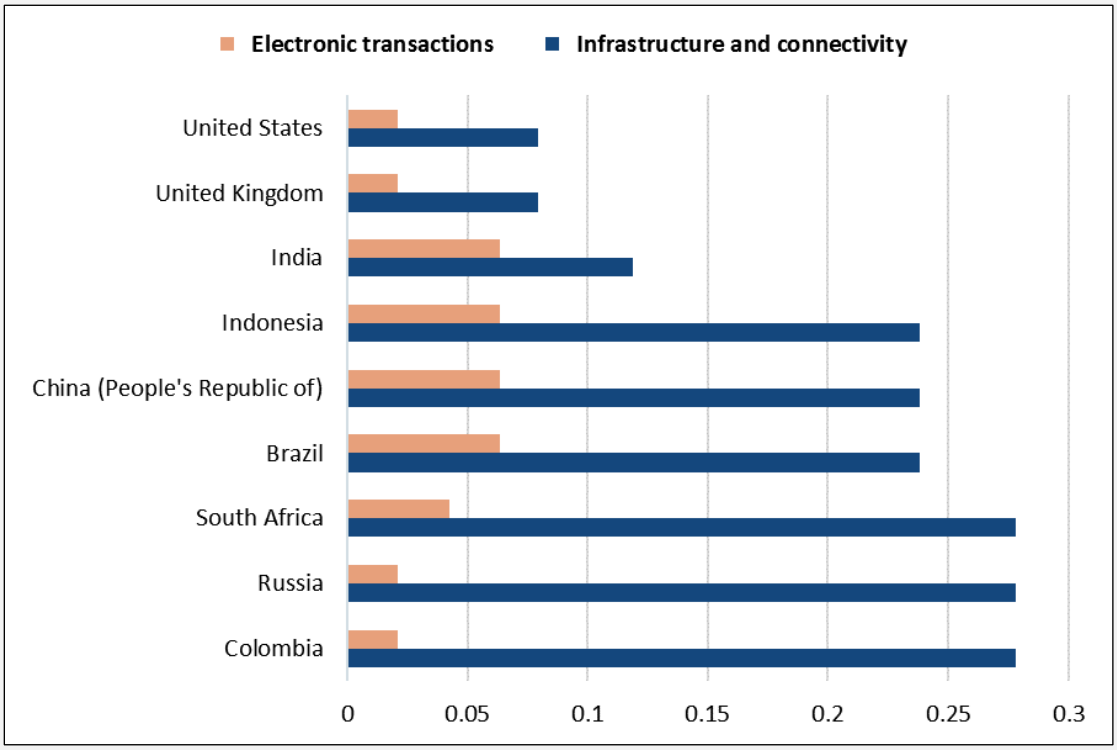
[17] Ferencz, J., "The OECD Digital Services Trade Restrictiveness Index", OECD Trade Policy Papers, No. 221, OECD Publishing, Paris, 2019, https://doi.org/10.1787/16ed2d78-en and https://stats.oecd.org/Index.aspx?DataSetCode=STRI_DIGITAL#.

[18] Electronic transactions in the index are defined as: issues such as discriminatory conditions for issuing licenses for e-commerce activities, the possibility for online tax registration and declaration for non-resident firms, deviation from internationally accepted rules on electronic contracts, measures inhibiting the use of electronic authentication (such as electronic signature), and the lack of effective dispute settlement mechanisms. Other policy areas of the Digital STRI cover infrastructure and connectivity, payment systems, intellectual property rights, and other barriers.

[19] Infrastructure and connectivity in the index relates to communication infrastructures essential to engaging in digital trade, including the extent to which best practice regulations on interconnections among network operators are applied to ensure seamless communication. Measures limit or block the use of communications services like Virtual Private Networks or leased lines or policies that affect connectivity such as cross-border data flows and data localization rules.

[20] Jan Lindenau, "Russia's Sovereign Internet Law Comes Into Force," *The Moscow Times*, November 1, 2019. For full text of "On Information, Information Technologies, and Protecting Information" see: http://publication.pravo.gov.ru/Document/View/0001201905010025.

Figure 3. Digital Services Trade Restrictiveness for Selected Countries



Source: CRS, based on OECD data, https://stats.oecd.org/?datasetcode=STRI_DIGITAL.

Varying policy approaches and the lack of global rules and consensus have resulted in a diversity of digital trade rules that will grow in complexity as the digital economy expands. Some analysts predict that the inconsistencies and diversity in rules and regulations may create hard splits between different dataspheres leading to digital trading blocs. Ongoing e-commerce negotiations at the WTO aim to set a common foundation of trade rules and disciplines and could lead to interoperability mechanisms to build bridges between differing internet regimes. While internet policies evolve at national levels and WTO e-commerce negotiations are ongoing, multiple international forums are discussing internet governance issues with active participation from the U.S. public and private sector. These forums often may identify best practices, principles, and frameworks but do not necessarily lead to enforceable rules (see text **box International Discussions of Internet Norms**).

International Discussions of Internet Norms

- The **U.N. Office for Disarmament Affairs** leads discussions on international ICT-security. In this forum, China advocates internet-sovereignty and aims to influence global norms. Specifically, China asserts "States should exercise jurisdiction over the ICT infrastructure, resources as well as ICT-related activities within their territories," while at the same time contending that "States should work together to create a multilateral, democratic and transparent global Internet governance system."
- The **U.N. Internet Governance Forum** aims to be a platform for governments, companies, technical experts, and civil society to engage on internet and technology policy issues and work toward common principles. According to the U.N. Secretary-General, it will also appoint a "technology envoy to work with governments, industry and civil society to help advance international frameworks."

- The **Organization for Economic Co-operation and Development (OECD)** provides an opportunity for member governments to cooperate in establishing international norms and standards, collecting and analyzing data, and sharing experiences and best practices. The OECD 1980 Privacy Guidelines established the first international set of privacy principles emphasizing data protection as a condition for the free flow of personal data across borders. This document serves as the basis for many national and international privacy policies and is referenced in recent U.S. trade agreements. Separate OECD committees are updating the privacy guidelines and negotiating rules for digital service taxes.
- The **G-20**, under Japan's leadership in 2019, launched a discussion of "data flows with trust." The Leaders' Declaration from the Osaka summit pledged international co-operation to "encourage the interoperability of different frameworks" and reaffirmed the "importance of interface between trade and digital economy." Twenty-four participants, including from the United States, Europe, China, and Russia, signed the final declaration on the digital economy, which supported international policy discussions, including ongoing negotiations at the WTO (see "WTO Plurilateral E-commerce Negotiations"). Notably, G-20 members India, Indonesia, and South Africa did not sign the declaration.
- The **Asia-Pacific Economic Cooperation (APEC)** is a cooperative economic forum for both governments and industry to share best practices and set high-level principles on issues that may be of greater concern to developing countries with less advanced digital economies and industry, such as using ICT to drive economic growth and social development.

  To address personal data privacy concerns, APEC is implementing its Cross-Border Privacy Rules (CBPR) system to establish a common set of rules to bridge differences that may exist among domestic privacy approaches. The system currently has eight member countries, including the United States, and could serve as a model for how countries can create interoperability across divergent internet regimes.

U.S. and Major Trading Partners' Internet Regimes

U.S. Approach

Maintaining a global network that is open, interoperable, reliable, and secure is a stated policy priority for the U.S. government.[21] Some Members of Congress have introduced bills supporting an open internet and expanded global internet access (see, for example, H.R. 600 and H.R. 739).

Congress recognized these priorities with respect to trade in its enhanced digital trade policy objectives for U.S. trade negotiations in the Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (P.L. 114-26), or Trade Promotion Authority (TPA), signed into law in June 2015.[22] The proposed USMCA made progress on these objectives, establishing a legal framework for an open North American digital economy that ensures cross-border data flows and protects consumers and data privacy, among its many provisions.[23]

Under the proposed USMCA, the United States, Mexico, and Canada agreed to a common set of digital trade rules, which may serve as a template for future U.S. FTAs. According to USTR, the new U.S.-Japan digital trade agreement, signed in October 2019, "meets the gold standard on digital trade rules set by the USMCA."[24] The provisions in the USMCA and U.S.-Japan

[21] https://www.state.gov/internet-freedom/.

[22] For more information on TPA, see CRS In Focus IF10038, *Trade Promotion Authority (TPA)*, by Ian F. Fergusson.

[23] The USMCA Digital Trade chapter is available at: https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.

[24] USTR, "FACT SHEET: U.S.-Japan Trade Agreement," September 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/september/fact-sheet-us-japan-trade-agreement. The U.S. Japana digital trade agreement is available at: https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concernin

agreement build on the digital trade rules agreed under the proposed Trans-Pacific Partnership (TPP), now in force under the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP or TPP-11) among 11 countries, not including the United States. Mexico, Canada, and Japan are all members of the TPP-11.[25] The TPP-11 rules have some clear differences from those in EU or Chinese FTAs.[26] For example, the TPP-11 agreement provisions ensure open cross-border data flows while EU and Chinese FTAs exclude similar provisions.

Protecting a Free and Open Internet as a U.S. Policy Priority

"The United States will advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services. The United States will promote the free flow of data and protect its interests through active engagement in key organizations, such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), the U.N., and the International Telecommunication Union (ITU)." [27] – The White House, *National Security Strategy of the United States of America*.

No single federal entity has primacy on all aspects of the digital economy, and the United States has not taken a holistic domestic approach to regulating the digital economy or governing the internet. As noted for a congressional hearing on internet architecture and the multiple federal agencies involved in safeguarding it domestically, unlike some other countries, "the [U.S.] government does not manage the internet, nor direct its use, but rather sets the laws, policies, and procedures for the private sector, academia, and individuals to follow in their use of the internet."[28]

The United States and China are the lead economies setting and attempting to export their rules and are often seen as the two ends of the policy spectrum. Other countries are forming national approaches that reflect their own domestic priorities.

The People's Republic of China (PRC)

China presents a number of significant opportunities and challenges for the United States in digital trade. China aims to be a "cyber superpower," and its trade and internet policies reflect state direction and industrial policy, limiting the free flow of information and individual privacy and discriminating against foreign companies. The Chinese government has sought to advance its views on how the internet should be expanded to promote trade, but also to set guidelines and standards over the rights of governments to regulate and control the internet, a concept it has termed "Internet Sovereignty."[29] The Chinese government appears to have first advanced a policy

g_Digital_Trade.pdf.

[25] CPTPP includes Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.

[26] In January 2017, the United States withdrew from the TPP. For more information on the CPTPP, see CRS In Focus IF10000, *TPP: Overview and Current Status*, by Brock R. Williams and Ian F. Fergusson.

[27] The White House, *National Security Strategy of the United States of America*, December 2017, p. 41, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[28] House Oversight and Reform subcommittee on National Security Committee Staff, *House Oversight Subcommittee Issues Hearing Memo on Securing the Nation's Internet Architecture*, September 4, 2019. U.S. Congress, House Committee on Oversight and Reform, Subcommittee on National Security, and House Armed Services Committee, Subcommittee on Intelligence & Emerging Threats & Capabilities, *Securing the Nation's Internet Architecture*, 116th Cong., September 10, 2019, https://armedservices.house.gov/2019/9/securing-the-nation-s-internet-architecture.

[29] Originally, China appeared to be mainly focused on establishing the rules of the road for the Internet in China, but over the past few years it appears to be advancing its vision of Internet sovereignty globally.

of "Internet Sovereignty" around June 2010, when it issued a white paper titled "the Internet of China," which stated the following:

> Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security.[30]

Analysts characterize "cyber sovereignty" or "internet sovereignty" as an organizing principle of internet governance that contrasts with the U.S. support for a global, open internet.[31] As one analyst stated, "the Chinese internet governance model is the first real challenge to a free and open internet."[32] China is clear in its position that:

> the principle of sovereignty… also includes cyberspace. Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing.[33]

A multitude of Chinese rules and initiatives illustrates the government's efforts to achieve cyber sovereignty. China benefits from a tightly controlled domestic system that not only allows the government to maintain strict controls on information dissemination, but also protects its market to the advantage of Chinese domestic economic players. When compared with the United States, China does not clearly separate the state from the economy. In 2016, citing national security justifications, China released its National Cybersecurity Strategy Report, which stated that its authorities would "firmly defend the cyber sovereignty of China using all means including economic, administrative, scientific, legal, diplomatic and military ways."[34]

China's state control over the internet and its use of digital technologies to control its domestic population, including through extensive digital surveillance and harvesting of big data for its social credit system, has been termed "digital authoritarianism" (see text box **U.S. Policy and Chinese Digital Authoritarianism**). The PRC social credit system includes two connected but distinct systems: a system for monitoring individual behavior, still in the pilot stages, and a more robust system for monitoring corporate behavior. Each firm's social credit profile is the aggregate of potentially hundreds of data points compiled into a central database developed by China's National Development and Reform Commission. Data disclosure requirements under the new social credit system may obligate firms to provide the Chinese government with sensitive data, such as personnel information or technological know-how.[35] Multinational firms in China are already subject to the system's data reporting requirements; they have raised concerns that certain provisions and rating criteria could be used to discriminate against multinational firms (including

[30] The People's Daily, *Full Text: The Internet in China*, June 8, 2010, available at http://en.people.cn/90001/90776/90785/7017202.html.

[31] Adam Segal, "When China Rules the Web," *Foreign Affairs*, September/October 2018.

[32] Joseph Bernstein, "The American Internet Sucks. The Alternative Is China." *Buzzfeed News*, November 17, 2019.

[33] Ibid.

[34] "China Vows to Protect Information Security 'Using All Means'," *Bloomberg News*, December 27, 2016.

[35] European Union Chamber of Commerce in China, "The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors," September 2019, https://www.europeanchamber.com.cn/en/publications-archive/709/The_Digital_Hand_How_China_s_Corporate_Social_Credit_System_Conditions_Market_Actors

for political purposes) lead to a more opaque market access regime, and increase compliance costs.[36]

U.S. Policy and Chinese Digital Authoritarianism

In general, digital authoritarianism describes a government's attempt to control its citizens through technology.[37] U.S. concerns about Chinese digital authoritarianism extend beyond international trade. The U.S. National Cyber Strategy refers to China as a strategic adversary and states, "We will also work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism." (Pillar IV)

Congress has expressed an interest in understanding Chinese digital authoritarianism and its potential implications.[38] During a House Intelligence hearing, witnesses noted that the Chinese Communist Party (CCP) uses technology-augmented authoritarianism to protect national security, broadly defined as ensuring an absence of threats, real and perceived, to the CCP. [39]

China's so-called "Great Firewall" censors or blocks many foreign websites or mobile apps, as well as content the government considers subversive. According to Freedom House, a U.S.-based non-governmental organization, China was the worst abuser of internet freedom in 2018.[40] Differences between what U.S. and Chinese users can access on the same online platforms furthers the split of the Chinese internet regime from the rest of the world and raises concerns about access to information and freedom of speech.

China's national internet governance regime is underscored by its recently-passed Cybersecurity Law, as well as other regulations that raise a variety of concerns for U.S. firms doing business in China. For example, companies are obliged to provide the government with full access to their proprietary data, if requested. The law's rules include requirements for:

- storing data locally and limiting cross-border data flows;
- cybersecurity testing and reviews of "critical network equipment" and "critical information infrastructure" operators by government authorities; and
- the use of "secure and controllable" technology in certain sectors mandating suppliers purchase Chinese products among other limitations.[41]

Fearing they could potentially lose control of their intellectual property and proprietary data, many U.S. firms have opted not to enter or faced constraints to remain in the Chinese market.[42]

---

[36] For more information, see CRS In Focus IF11342, *China's Corporate Social Credit System*, by Michael D. Sutherland.

[37] Freedom House, "Freedom on the Net 2018 The Rise of Digital Authoritarianism," October 2018, p. 2,https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

[38] The National Cyber Strategy of the United States of America states that the United States will "work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism." White House, National Cyber Strategy of the United States of America, September 2018, available at https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[39] U.S. Congress, House Permanent Select Committee on Intelligence, *China's Digital Authoritarianism: Surveillance, Influence, and Political Control*, 116th Cong., May 13, 2019.

[40] Freedom House, "Freedom on the Net 2018 The Rise of Digital Authoritarianism," October 2018, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

[41] The Cybersecurity Law was passed by the government on November 7, 2016 (effective June 1, 2017), with continued refinement through implementing regulations.

[42] Based on CRS conversations with American Chamber of Commerce in the People's Republic of China (AmCham China), August 2019.

Some foreign firms with customers in China try to address concerns about potential government access to their proprietary data by segregating data transiting to or through China from the rest of their business. This may require U.S. firms to partner with local Chinese firms such as through joint ventures. For example, Apple is unable to offer many of its newer services within China and its iCloud service is available only through a local government-backed provider.[43]

China's policies also raise concerns among some U.S., EU, and other government officials and company executives about Chinese companies operating overseas or on a cross-border basis using business models that give Chinese firms access to sensitive data. If Chinese companies need to follow domestic Chinese laws and Chinese government directives, U.S. and other officials fear that sensitive data involving their citizens and corporate entities could be exposed to the Chinese government.

China also exports domestically-produced technologies, including security cameras, telecommunications hardware, and internet filtering software, to other countries where governments may seek not only to increase security but also to exert greater control over populations and contain internal dissent.[44] Analysts disagree as to whether China is aggressively exporting digital authoritarianism as an overarching internet governance system, including sales of the enabling technologies and underlying infrastructure to potentially provide Chinese authorities access to data. The alternative is that China is simply promoting domestic industry exports. Regardless of intent, the results in countries that import Chinese goods, services, and policies show how China's technology exports are expanding the country's influence in ICT markets and international standards forums in ways that advance Chinese goals and norms.

China also uses its domestic technical standards to separate itself from the broader international community. China, for example, exports its ICT products and services, as well as its technology standards, through projects under its Belt and Road Initiative and, in particular, its Digital Silk Road.[45] China promotes indigenous innovation of technology and investment in domestic research and development projects (R&D) in emerging technologies like artificial intelligence and fifth-generation telecommunications (5G), the future backbone of the internet of things (IoT). Procurement contracts in China require or prefer domestic standards to international ones and/or require domestic production of ICT equipment. In recent years, China has increased its participation in international standards-setting bodies such as the International Organization for Standardization (ISO); its assumption of leadership positions in these organizations illustrates China's efforts to balance its isolationist tendencies and cyber-sovereignty policies with the potential economic gain that comes from international engagement and shaping global standards (see "Standards Development").

European Union (EU)

The EU approach to internet governance, including digital trade, is less state-controlled than China's internet regime, but more regulatory and prescriptive than the current U.S. approach. The

[43] Mark Gurman, "Apple TV+, Apple Arcade, Other Apple Services Blocked in China," *Bloomberg*, November 7, 2019.

[44] Paul Mozur, et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019.

[45] China's Belt and Road Initiative (BRI) aims to boost economic connectivity across continents by land and by sea. Under the initiative, PRC institutions are financing transportation and energy infrastructure projects in dozens of countries and PRC government agencies are working to reduce investment and trade barriers and boost people-to-people ties.

EU seeks to establish itself as a technology leader and set its own mark on global internet norms. EU Commission president Ursula von der Leyen outlined her priorities for her new executive vice-president for a digital age and stated, "[w]e have to work hard on technological sovereignty."[46]

The EU Council's June 2019 strategic agenda echoed these sentiments:

> We need to ensure that Europe is digitally sovereign and obtains its fair share of the benefits of this development. Our policy must be shaped in a way that embodies our societal values, promotes inclusiveness, and remains compatible with our way of life. To this end, the EU must work on all aspects of the digital revolution and artificial intelligence: infrastructure, connectivity, services, data, regulation and investment. This has to be accompanied by the development of the service economy and the mainstreaming of digital services.[47]

The same document refers to the need for a level playing field in trade and highlights the importance of "ensuring fair competition, reciprocity and mutual benefits" in trade policy.[48] The EU will need to balance its goals of achieving technological sovereignty without isolating the region to achieve gains from expanded international trade that require interoperability and open access and data flows.

An EU Commission document frames Europe's technological sovereignty, itself an emerging and undefined term, as an initiative within a broader EU industrial strategy. The document specifically tasks the new executive vice president with "striving for digital leadership" while preserving the "European way."[49] EU officials characterize the region's internet regime as a third way between those of the United States and China. Some in the EU support a policy of cyber sovereignty and an independent European internet architecture. As one commentator stated, "If there is an American internet and a Chinese internet, there should also be a European one — a framework in which Europeans can make their own decisions about data and privacy, free expression and state security, and taxation and competition."[50]

Critics see the EU's desire for internet sovereignty as driven by protectionist and anti-competitive motives to incubate and grow European champions in the digital sphere that can effectively compete against large U.S. and Chinese internet firms.[51] Others view the EU effort less antagonistically, noting German chancellor Angela Merkel's statement that "we need to commit ourselves to protecting the core of the internet as a global, public good."[52] Merkel clarified her vision of European cyber sovereignty stating, "on the one hand, we want to preserve our digital sovereignty while on the other hand, we don't want to isolate ourselves but act multilaterally… In my understanding, digital sovereignty does not mean protectionism or state authorities deciding what kind of information can be disseminated — which is censorship — but it rather describes the capability to shape the digital transformation, both as an individual and as a society."[53]

---

[46] Mark Scott, "Margrethe Vestager's vast new powers," *PoliticoPro*, September 10, 2019.

[47] European Council, Council of the European Union, *A new strategic agenda 2019-2024*, June 20, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/.

[48] Ibid.

[49] European Commission, "Executive Vice-President-designate for a Europe fit for the Digital Age," September 10, 2019.

[50] Philip Stephens, "Europe Must Set its Own Digital Rules," *Financial Times*, August 8, 2019.

[51] Christian Borggreen, "European 'tech sovereignty' or 'tech protectionism'?," *Disco*, October 30, 2019.

[52] Janosch Delcker, "Merkel: Democracies must join forces to protect a free internet," *PoliticoPro*, November 26, 2019.

[53] Ibid.

In defining the "European way," the EU has set precedents in some areas of the digital economy. Examples of major EU digital initiatives with global implications that may impact U.S. firms doing business in the EU include the following:

- **EU General Data Protection Regulation (GDPR)**. The GDPR, which took effect on May 25, 2018, establishes a set of binding and enforceable rules for the protection of personal data throughout the EU. The GDPR seeks to strengthen individual fundamental rights and facilitate business by ensuring more consistent implementation of data protection rules EU-wide. With no multilateral rules on cross-border data flows, some experts contend that the GDPR may effectively set new global data privacy standards, since many U.S. and foreign companies and organizations are striving for GDPR compliance to avoid being shut out of the EU market, fined, or otherwise penalized. In addition, some countries outside of Europe (e.g., Brazil) are imitating all or parts of the GDPR in their own privacy regulatory and legislative efforts whether on their own initiative or at the EU's behest.[54]
- **Cloud-hosting Services.** The German Economy Ministry, with support from other EU leaders, is working to develop a cloud-hosting service (Gaia-X) to provide European government agencies and companies a European alternative to U.S. and China-based cloud service providers, such as Amazon Web Services or Microsoft. According to the ministry, the aim is to ensure European users that the data is "sovereign" and not subject to potential (mis)use by foreign law enforcement or intelligence services, or being blocked for political reasons such as a trade dispute.[55] In a similar effort to limit its current dependence on U.S. technology companies, France's Interior Ministry is planning to offer an internal government cloud service known as Nextcloud.[56]
- **Digital Single Market (DSM).** EU policymakers are attempting to bring more harmonization across the region and break down barriers among EU countries under the DSM initiative. The DSM is an ongoing effort to unify the EU market, facilitate trade, and drive economic growth through technology and digital trade. The EU has rolled out multiple initiatives and rules under the DSM, with which any firm doing business in the EU must comply. It is not clear how the DSM initiatives will align with U.S. policy and norms. For example, a new Digital Services Act will provide for uniform rules for online platforms and digital services, including rules on intermediary liability, updating various sets of existing rules in the EU. Others stakeholders raise concerns that platform regulation may limit competition and favor EU entities.
- **Digital Services Taxes (DSTs)**. Several countries in Europe, and the European Commission, have proposed or adopted taxes on revenue earned by multinational corporations (MNCs) in certain "digital economy" sectors from activities linked to the user-based activity of their residents. These proposals have generally been labeled as DSTs. Proponents of DSTs argue that digital firms are "undertaxed."

[54] For example, see Covington & Burling, LLP, "Brazil's New General Data Privacy Law Follows GDPR Provisions," August 20, 2018. For more information on the GDPR, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

[55] Janosch Delcker, "Germany's plan to control its own data," *PoliticoPro*, September 12, 2019.

[56] Samuel Stolton, "Altmaier's cloud initiative and the pursuit of European digital sovereignty," *Euractiv*, August 29, 2019.

> U.S. critics, in particular, see DSTs as an attempt to target U.S. tech companies, especially as minimum thresholds are high enough that only the largest digital MNCs, which tend to be American, would be subject to the tax.[57] Without a multilateral agreement or an EU-wide rule, DST policies vary across European countries. Countries outside the EU, such as Canada, are also considering implementing a DST.[58] Some countries are implementing domestic DSTs while multilateral negotiations on digital service taxes are occurring under the Organization for Economic Co-operation and Development (OECD).[59]

These EU initiatives may add to current heightened tension in the U.S.-EU trade and economic relationship. New U.S.-EU trade negotiations could de-escalate tensions and address internet governance issues, but no agreement exists on the scope of potential bilateral trade negotiations although discussions continue.[60]

Despite common rules across the EU, the United Kingdom's (UK's) future internet regime after the country's withdrawal from the EU ("Brexit") is unclear. The UK has stated that it will continue to follow GDPR, but would need an adequacy decision by the EU to prevent disruptions to the free flow of personal data between the EU and the UK. Without such a decision, individual organizations would have to use other means specifically approved by the EU to transfer personal data between the UK and EU (e.g., standard contractual clauses). The EU is set to evaluate the UK data protection framework in 2020.[61] UK leaders seek regulatory autonomy from the EU post-Brexit in some areas and alignment with the EU in others, but it is not clear if and how potential UK regulatory changes would affect internet policy or if any changes by the UK would align it more closely with U.S. policy.[62] Differences in U.S. and UK internet policies will likely need to be addressed in any future bilateral trade negotiations.

Other Approaches

While some countries may use the U.S. or Chinese approach to internet governance as a model, often they seek to balance these influences with their own domestic policies and priorities. Across the spectrum between U.S. and Chinese internet policies lie a variety of national policies neither as open as the former nor as closed as the latter. Other countries often wish to retain trading and investment relationships with both U.S. and Chinese partners. India and Vietnam illustrate two such examples.

India

India is seeking to become a technology leader and has asserted itself on the international stage while protecting its domestic industries. On the one hand, India seeks to aggressively export

[57] For more information on digital services taxes, see CRS Report R45532, *Digital Services Taxes (DSTs): Policy and Economic Analysis*, by Sean Lowry.

[58] Canada Office of the Parliamentary Budget Officer, "Cost Estimate of Election Campaign Proposal Taxation of large technology companies," September 29, 2019.

[59] For more information on OECD tax negotiations, see http://www.oecd.org/tax/.

[60] For more information, see CRS In Focus IF11209, *Proposed U.S.-EU Trade Agreement Negotiations*, by Shayerah Ilias Akhtar, Andres B. Schwarzenberg, and Renée Johnson.

[61] Saqib Shah, "UK, EU deal includes close cooperation on data protection, cybersecurity," *Bloomberg*, October 17, 2019.

[62] For more information, see CRS In Focus IF11123, *Brexit and Outlook for U.S.-UK Trade Agreement*, by Shayerah Ilias Akhtar.

technology services and prioritizes opening access to foreign markets for specific types of services in trade negotiations so that Indian technology workers can work abroad.

On the other hand, India uses protectionist rules and regulations to shield its domestic industry from foreign competition. For example, India's draft e-commerce policy is intended to favor domestic entities through requirements for local data storage and national standards, among other provisions.[63] Additional policies under consideration by the Indian government would restrict international e-commerce platforms operations and would require them to adjust their supply chains.[64] India has cited security as the rationale for its draft Personal Data Protection Bill, which would also establish broad data localization requirements and limit cross-border transfer of some data.[65] At times, India has taken steps to curb internet freedom, such as temporarily shutting down mobile networks or blocking social media apps in certain regions, justifying such as actions as an attempt to halt disinformation.[66]

Although India joined the WTO Information Technology Agreement to eliminate tariffs on ICT goods such as multi-component semiconductors, it has since begun imposing tariffs on some ICT imports. The EU filed for consultation with India over the tariffs in 2019, the first step in WTO dispute settlement.[67] The United States and five other WTO members have since joined the request.[68] In addition, India does not support extending the temporary WTO moratorium on tariffs on electronic transmissions that will expire in mid-2020.[69] India's ability to block a consensus decision to continue the moratorium may increase the pressure to address the topic in the ongoing WTO e-commerce negotiations. To date, India has elected not to participate in the plurilateral negotiations (see below).

Due to concerns about Indian market access restrictions on U.S. exports, in 2019, President Trump terminated India's eligibility for the U.S. Generalized System of Preferences (GSP), which gives duty-free tariff treatment to certain U.S. imports from eligible developing countries to support their economic development. To address frictions in the trading relationship, the two countries began bilateral trade discussions to address key U.S. concerns regarding access to India's market. Negotiations are ongoing and it is unclear whether they will address nontariff barriers to digital trade, such as data localization requirements and other internet rules.[70]

Vietnam

Vietnam is adopting elements of the Chinese internet approach in some policy areas. For example, in June 2018, Vietnam passed its Law on Cybersecurity with requirements for data

[63] Newley Purnell, "India Increases Pressure on Amazon and Walmart," *The Wall Street Journal,* February 25, 2019.

[64] Newley Purnell, "U.S. Tech Giants Bet Big on India. Now It's Changing the Rules," *The Wall Street Journal*, December 3, 2019.

[65] INDUSLaw, "India: The Debate – Data Localization And Its Efficacy," September 17, 2018, mondaq.com.

[66] Freedom House, "Freedom on the Net 2018 The Rise of Digital Authoritarianism," October 2018, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

[67] WTO DS582: India — Tariff Treatment on Certain Good in the Information and Communications Technology Sector, April 2, 2019.

[68] WTO WT/DS582/4. For more information, see https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds582_e.htm.

[69] Press Trust of India, "India, SA ask WTO to review moratorium on e-commerce customs duties," *Business Standard*, June 4, 2019.

[70] For more information, see CRS In Focus IF10384, *U.S.-India Trade Relations*, by Shayerah Ilias Akhtar and K. Alan Kronstadt.

localization and access to information by Vietnamese authorities on the grounds of national security, among other provisions.[71]

At the same time, Vietnam is liberalizing its economy and seeking to gain from the U.S.-China trade war as U.S. companies relocate their supply chains from China to other nearby Asian destinations. To spur economic growth and integration, Vietnam joined TPP-11, which went into effect in January 2019. However, the country has a two-year grace period before being subject to dispute settlement for parts of the e-commerce chapter, including provisions on cross-border data flows and localization prohibitions.[72] U.S. firms and others will be watching to see how Vietnam reconciles its current restrictive internet with its TPP-11 commitments for open data flows. Vietnam could, for example, create carve-outs or relax the requirements of its cybersecurity regulations, or it could maintain the rules and claim national security as a legitimate public policy objective and exemption under TPP-11.

Vietnam also appears to be aligning with the United States in the telecommunications sector. For example, Vietnamese providers are refraining from purchasing 5G equipment from Chinese suppliers, noting concerns voiced by U.S. cybersecurity officials (see text box **Standards, 5G, and National Security**). The Vietnamese government has not taken a formal position in favor of western or Chinese telecommunications equipment and standards.[73]

WTO Plurilateral E-commerce Negotiations

Background: Digital Trade Rules

Trade negotiations are a tool to create binding and enforceable rules and disciplines to promote international trade and bridge differing internet regimes. No comprehensive agreement on digital trade exists in the WTO as the General Agreement on Trade in Services (GATS) entered into force in January 1995, before the explosive growth of global data flows and digital trade. [74]

Initially, digital trade was a niche concern, primarily focused on trade in ICT goods and e-commerce. Certain WTO agreements cover some aspects of digital trade, such as the WTO Information Technology Agreement (ITA) on tariffs. As noted, since 1998, WTO members have also agreed to a moratorium on customs duties for electronic transactions.[75] Although the ban is temporary it has been continuously renewed, most recently until the next ministerial conference in June 2020.[76] As the WTO ITA and e-commerce moratorium illustrate, multilateral trade negotiations to date focused mainly on tariffs and non-discrimination, as well as broad statements of cooperation. Non-tariff barriers were broadly left unaddressed and standards development were left to technicians and academia. As internet-connected technologies continue to evolve, many emerging areas still lack common definitions, standards, and metrics. Today, standards

[71] Yee Chung Seck and Thanh Son Dang, "Vietnam National Assembly Passes the Law on Cybersecurity," Global Compliance News, July 2, 2018.

[72] CPTPP, Chapter 14, Article 14.18.2.

[73] Raymond Zhong, "Is Huawei a Security Threat? Vietnam Isn't Taking Any Chances," *New York Times*, July 18, 2019.

[74] For more information, see CRS Report R44565, *Digital Trade and U.S. Trade Policy*, coordinated by Rachel F. Fefer.

[75] WTO, *Declaration on Global Electronic Commerce Adopted on 20 May 1998*, WT/MIN(98)/DEC/2, May 25, 1998.

[76] WTO General Council, *Work Programme on Electronic* Commerce, WT/L/1079, December 10, 2019.

conversations attract a wide range of stakeholders and WTO plurilateral negotiations provide an opportunity to set new international rules and disciplines for digital trade.

Recent bilateral and plurilateral trade agreements have begun to incorporate commitments on the digital economy, adding to the complex mixture of international trade rules that companies must follow. Although the various FTAs differ in their scope and participants, their provisions can provide ideas and templates for broader WTO negotiations. While not every country participates in an FTA with digital trade rules, all countries are involved in the digital economy and have a stake in shaping its future growth.

Over 75 countries, including the United States, are participating in ongoing WTO e-commerce negotiations aiming to establish a global framework and obligations that enable digital trade in a nondiscriminatory and less trade restrictive manner. Participants released the Joint Statement on Electronic Commerce at the 11th WTO Ministerial Conference in December 2017 announcing their intent to "initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce."[77] Australia, Japan, and Singapore are coordinating the initiative, known as the Joint Statement Initiative or JSI and participants include both developed and developing countries. Negotiations began in January 2019, initially focused on information exchanges, education, and outreach, especially to developing country members who expressed interest but may not yet have developed a clear domestic digital trade agenda or policy.

Multiple parties have submitted proposals outlining their positions and desired scope for the negotiations.[78] The proposals reflect the diversity and evolving state of internet regimes globally. Some developing countries have opted not to participate, including India and South Africa, who want to protect their flexibility and policy space. These parties may not want to commit to an agreement that may constrain their efforts to incubate, or protect, domestic industry or to raise potential tariff revenue on digital products. However, it is not clear why some countries, such as Vietnam, that have agreed to digital trade commitments in other FTAs (such as TPP-11) are not taking part, though they may do so later.

Positions among Major Participants

The **United States** was one of the first parties to submit an initial discussion paper for the WTO e-commerce talks. The U.S. discussion paper includes "trade provisions that represent the highest standard in safeguarding and promoting digital trade" and reflects the U.S. support for a market-driven, open, interoperable internet under a multi-stakeholder system.[79] The paper builds on and enhances many of the commitments contained in TPP/TPP11 that were further refined in USMCA. Key provisions in the U.S. proposal include trade rules to:

- protect cross-border data flow and prevent data localization mandates;
- ensure fair treatment of digital products;
- protect proprietary information, including protecting source code and prohibit forced technology transfer;
- collaborate on cybersecurity; and

[77] Ministerial Conference, , *Joint Statement on Electronic Commerce*, WT/MIN(17)/60, December 13, 2017, available at https://ustr.gov/sites/default/files/files/Press/Releases/Joint%20Statement%20on%20Electronic%20Commerce.pdf.

[78] All proposals can be found on the WTO online documents portal: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx.

[79] United States, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/5, March 25, 2019.

- facilitate internet services and trade.[80]

For financial services, the proposal includes the same compromise included in the USMCA to prohibit data localization, provided that regulators have adequate access. The U.S. proposal also includes the USMCA provisions requiring that parties adopt or maintain a legal framework to protect personal information and encourages the development of interoperability mechanisms, though it does not specifically reference the APEC work on privacy. In line with recent U.S. FTAs, the U.S. proposal includes protecting internet intermediaries from liability for hosting content, a topic of ongoing congressional debate.[81]

China's proposal focuses on facilitating e-commerce and global value chains as a means to help WTO members, especially developing countries, benefit from digital trade. It reflects its state-driven model.[82] In contrast to the U.S. desire for an ambitious, high-standard agreement, China believes negotiations should "set a reasonable level of ambition" given members' varying levels of industry development, as well as historical and cultural traditions. China advocates respect for parties' differing policies on internet sovereignty, data security and privacy protection, and wants to allow for other regulatory measures to achieve "reasonable public policy objectives." In China's view, data flows, data storage, and treatment of digital products should be subjects for exploratory discussions rather than solid commitments. Development needs like bridging the digital divide and capacity building are highlighted throughout the Chinese proposal. Seemingly in response to U.S. restrictions on trade with Chinese firms such as Huawei, a second proposal from China focuses on preventing members from limiting or blocking trade in ICT equipment and products.[83] China's proposal reflects its visions of a world with separate national internets, in which international agreements allow sovereign states to maintain control and impose additional restrictions on firms within their borders. The limited overlap between the U.S. and Chinese proposals illustrates the difficulties negotiators will need to overcome to achieve a meaningful outcome.

The **EU** proposal falls between the U.S. and Chinese proposals.[84] The EU seeks a "comprehensive and ambitious set of WTO disciplines and commitments" including provisions on e-commerce, consumer and personal data protection, and intellectual property protection. The EU advocates revising the outdated WTO Reference Paper on Telecommunications Services to better promote competition, something not mentioned in the U.S. proposal.[85] The proposal also reflects the EU domestic policy emphasis on protecting personal privacy. Though the EU proposes allowing cross-border data flows and prohibiting localization requirements, it also allows members to "adopt and maintain the safeguards they deem appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data." Some analysts see the exception as nullifying the commitment to cross-border data flows.

Other countries have put forth proposals reflecting their own domestic policies. The majority of proposals seek to extend the moratorium on duties on electronic transmissions and contain

[80] United States, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/23, April 26, 2019.

[81] For more information on internet intermediary liability, see CRS Report R45650, *Free Speech and the Regulation of Social Media Content*, by Valerie C. Brannon.

[82] China, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/19, April 23, 2019.

[83] China, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/40, September 23, 2019.

[84] European Union, *Joint Statement on Electronic Commerce*, WTO INF/ECOM/22, April 26, 2019.

[85] WTO Telecommunications Services Reference paper, April 24, 1996, https://www.wto.org/english/news_e/pres97_e/refpap-e.htm.

provisions on consumer protection and security. In general, the proposals represent an attempt to bridge the limited Chinese and open U.S. proposals.

Industry in general supports the ongoing plurilateral negotiations as a means both to attain enforceable rules and provide the certainty needed for business operations and to expand international trade. One international coalition of information technology industry groups, for example, published its priorities for the negotiations including: open cross-border data flows, prohibiting tariffs and taxes on data flows and ICT goods, protection of source code, algorithms, and encryption, among other provisions.[86] The Global Services Coalition similarly endorsed the WTO e-commerce negotiations to promote trade in services and digitally enabled services.[87] In general, the USMCA, U.S.-Japan agreement, and U.S. proposal reflect the provisions sought by industry, with exceptions to achieve legitimate public policy objectives in a least trade-restrictive manner.

On the other hand, one coalition of civil society organizations opposes the ongoing WTO negotiations, believing that any agreement would favor large multinational technology companies at the expense of developing country entrepreneurs and workers.[88] Another civil society group stated that negotiations should focus on transparency, consumer protection and consumer rights, promoting competition, ensuring dispute resolution, and securing citizen access to their online data. It also warned, however, that data protection, privacy, net neutrality, artificial intelligence, and cybersecurity should not be part of a trade agreement.[89] Some consumer groups have engaged constructively with WTO representatives to advocate for transparency in the negotiations and multi-stakeholder dialogues.[90] A clear consensus among the consumer groups on how to address the issues of data privacy and data flows has yet to emerge.

Selected Issues and Challenges

The parties aim to streamline proposals into a common text ahead of the next WTO ministerial conference in Kazakhstan in June 2020. Given the diversity of the parties' positions and national regimes, the negotiations will need to address controversial issues to achieve a meaningful agreement. Some hope that significant progress and some level of political agreement are possible by then, although the parties will likely require more time to reach an agreement with meaningful and enforceable obligations.

Clear commonalities, as well as differences, appear among the proposals, foreshadowing likely controversies and challenges as the negotiations move forward. These include:

- **E-signatures, e-contracts, and related measures to facilitate e-commerce and protect consumers** will likely attract wide consensus from all parties.

[86] Information Technology Industry Council, "Global Industry Position Paper on the WTO E-Commerce Initiative," October 07, 2019.

[87] July 16, 2018, "Global Services Coalition Letter to WTO Ministers to Re-Double Efforts to Make Progress Toward a High Standard E-Commerce Framework," January 18, 2019.

[88] Civil Society Letter Against Digital Trade Rules in the World Trade Organization, April 1, 2019.

[89] Burcu Kilic, Ph.D., Director, Public Citizen Digital Rights Program, statement, October 31, 2019.

[90] https://www.wto.org/english/news_e/news19_e/summary_of_points_raised_trdia_06may19_e.pdf.

- The U.S., Chinese, and EU proposals all include an extension of the WTO temporary **moratorium on customs duties on electronic transmissions**, but their positions, as well as those of other members, vary as to whether it should be made permanent.[91]
- **Digital services taxes**, such as those in place in various EU countries and under consideration in some EU and non-European countries, may be addressed directly or could be excluded from the final trade agreement and left for ongoing OECD negotiations that cover broader international tax issues.
- The United States and some other parties seek broad protections for **cross-border data flows and prohibitions on data localization requirements**. Other parties support open data flows but under a narrower scope (e.g., for certain sectors or types of data) or with broader exceptions. As noted, China does not want to include any commitments related to data flows.
- **Personal data privacy** will be among the most difficult issues. While privacy preferences and rules affect trade, privacy policies and concerns are broader than international trade and trade agreements, for example, affecting medical or financial regulation. The agreement could also address interoperability mechanisms (e.g. certification schemes, contracts, or other data-specific agreements) in addition to or instead of identifying specific privacy protections or obligations.
- **Cybersecurity** provisions, if included, could include specific commitments to prohibit or allow certain actions or policies, or may focus on cooperation between the parties.

As in every negotiation, the parties must balance creating obligations to facilitate trade with respecting parties' sovereignty. Maintaining sufficient flexibility and policy space may be especially important for those members still determining their domestic digital agenda. Analysts expect that the plurilateral negotiators will have to decide between scope and inclusion. A narrow agreement with limited scope and provisions, such as those focused on e-commerce facilitation, would likely retain the greatest number of negotiating participants but could have less impact. On the other hand, a high-standard broad agreement with deeper commitments, such as that between the United States and Japan, may deter participants who are not yet willing or able to accept all the obligations. Possible approaches include the following.

A **staggered approach** or **early harvest** could allow the parties to reach an early consensus on some less controversial issues, potentially providing a basis for further rounds of negotiations. Such an agreement would provide an early "win" and establish a common framework for future negotiation, but may not have a high level of impact in countering trade barriers or bridging disparate internet regimes.

Some experts suggest a **tiered agreement** that contains provisions that all parties accept with additional voluntary commitments.[92] For example, all parties may be willing to accept binding commitments on the less controversial issues (such as e-signatures). Another tier with more ambitious provisions, such as prohibitions on data localization, could be agreed on a non-most favored nation (MFN) or reciprocity basis so that only the subset of parties that undertake the obligation would receive that benefit. For example, if country A agrees to no data localization requirements, it may still impose such requirements on countries that do not undertake the same commitment. This type of agreement would create a common framework, but would not

[91] Hannah Monicken, "Indonesia joins WTO e-commerce talks despite opposition to permanent moratorium," December 13, 2019.

[92] Based on CRS conversation with industry and government representatives.

necessarily prevent the splitting of the internet into different "dataspheres" if major economies do not adopt higher-standard provisions.

Interoperability mechanisms could be created under the auspices of the WTO or existing systems could be expanded to allow for open data flows between different cybersecurity or data privacy regimes.

Staged implementation and capacity building provisions have been included in other WTO agreements and may provide another way to provide flexibility and achieve both broad scope and inclusion. Such an agreement could allow certain parties, especially developing countries, more time to make domestic changes and implement commitments. Capacity building could also encourage all parties to commit to the more ambitious level of obligations. For example, the WTO Trade Facilitation Agreement (TFA) requires that "donor members" who do not require implementation assistance, such as the United States, provide the needed capacity building and support to developing and least-developed members. Members determine their own implementation schedules and progress in implementation is explicitly linked to technical and financial capacity. The TFA was the last concluded WTO multilateral agreement and implementation of members' commitments is ongoing.

Standards Development and Trade

Standards development and international standards, while not part of trade policy, are often referenced in trade agreements given that standards help shape market access. The growth of international trade in ICT goods and emerging technologies relies on interoperability and international standards. Traditionally, technology companies and telecommunication providers saw value in developing international standards that enable technology companies to build to one standard worldwide, bring products to market faster, sell equipment globally, achieve economies of scale, and reduce the cost of equipment. As technologies develop and converge, standards development becomes more complicated and participation and interest in the process grows. According to the WTO Technical Barriers to Trade Committee, WTO members are mandated to use relevant international standards as the basis for regulation, with some exceptions, and not create unnecessary obstacles to international trade.[93] U.S. FTAs refer to this "TBT Committee Decision on International Standards" in defining commitments on international standards. Using international standards encourages transparency, innovation, and flexibility; such standards can evolve as technologies and new best practices develop.

Today, SDOs that develop these international standards (e.g., International Organization for Standardization (ISO), 3rd Generation Partnership Project (3GPP)) are drawing attention not only from ICT sector and academic participants, but also from industries that rely on ICT goods and services as well as government organizations. Standards development illustrates the divergence between the U.S. and Chinese approaches to ICT.

China has a state-led approach to standardization. Under its Revised Standardization Law, effective in 2018, the Standardization Administration of China sets compulsory standards, but also endorses the adoption of international standards. In an effort to promote its industrial policies, develop domestic standards, and internationalize them, China has increased its participation in international standards development, especially for emerging technologies. While some stakeholders welcome China's participation, others question the benefits and risks of Chinese involvement in some of these forums. Some stakeholders raise concerns that China is

[93] WTO Technical Barriers to Trade Agreement Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards, https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm.

pursuing a strategic and nationalist, rather than market-driven and best-of-breed-technology, focus because of the Communist Party of China's interest in protecting and advancing its values on a world stage. Analysts have pointed out that China shows a preference for multilateral institutions such as the U.N. or WTO in which each country has a single vote rather than U.S.-backed multi-stakeholder standards institutions (SDOs) with a wider range of participants and more diverse views that dilute governments' clout.[94]

Debate over international versus Chinese standards, for example, has dominated many SDO discussions on emerging 5G networks as competition arises between Chinese and Western technology companies. China directs Chinese industry's participation in global SDOs--including leading technical committees, hosting forums, conducting 5G R&D, contributing to 5G specifications--and in international projects. China's industry and academic participants are state-controlled entities and typically work to institutionalize Chinese national standards at the global level.[95]

As a counterweight, some U.S. stakeholders advocate for increased participation by U.S. officials in SDOs and government resources for U.S. business and non-government participants to help maintain U.S. leadership in the development of emerging technologies. The Trump Administration echoed these sentiments in Executive Order (EO) 13859, stressing the importance of U.S. leadership in developing technical standards for AI.[96] In response, the National Institute of Standards and Technology (NIST) issued a plan for federal engagement in AI standards calling for the U.S. government to "commit to deeper, consistent, long-term engagement in AI standards development activities to help the United States to speed the pace of reliable, robust, and trustworthy AI technology development."[97]

Standards, 5G, and National Security

5G networks are expected to yield significant economic benefits by enabling providers to expand telecommunication services to consumers, governments, and industries. 5G is expected to support the growing number of connected devices, better integrate and optimize industrial technologies and processes, perform advanced data analytics, and enable the use of advanced technologies.[98]

With China actively engaged in technology standards discussions, including 5G, the Trump Administration and Congress have raised national security concerns over the use of foreign-made equipment in U.S. 5G networks, and global supply chains of advanced technology products. Potential issues related to the rollout of 5G technology and network development from a U.S. national security and intelligence standpoint include the legal leverage the China's intelligence services have over Chinese companies, among other concerns. The Chinese firm Huawei is one of three major 5G network equipment providers. Due to their legal obligations to the Chinese government, the U.S. government has subjected certain Chinese firms to particular scrutiny and export controls. For example, citing links with the Chinese government, the Administration has restricted U.S. entities from trading with Huawei

[94] Elsa Kania, "China's play for global 5G dominance—standards and the 'Digital Silk Road'," *Australian Strategic Policy Institute*, June 27, 2018.

[95] Anna Gross and Madhumita Murgia, "Chinese tech groups shaping UN facial recognition standards," *The Financial Times*, December 1, 2019.

[96] Executive Office of the President, "Maintaining American Leadership in Artificial Intelligence," 84 *Federal Register* 3967, 2019.

[97] NIST, U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools, August 2019, https://www.nist.gov/topics/artificial-intelligence/plan-federal-engagement-developing-ai-technical-standards-and-related.

[98] For more information on 5G or standards development and security concerns with specific Chinese firms, see CRS Report R45485, *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*, by Jill C. Gallagher and Michael E. DeVine.

and has urged allies not to work with the 5G supplier. The response from domestic technology firms and international partners has been mixed.[99]

One issue governments and analysts raise is that Administration actions could push Huawei and other Chinese-based firms to restrict their trade with U.S. companies, affecting U.S. jobs and revenues. It could also result in reducing China's dependence on Western technology, strengthening its own technology industry and ultimately hurting the U.S. and Western economies.

Issues for Congress

Given the critical and growing role of the internet to the U.S. economy, Congress has a policy and legislative interest in the current divergence in national internet regimes and its impact on digital trade, future trade negotiations, standards-setting, and other major U.S. policy objectives. Key issues for Congress include:

- Examining the U.S. position in the ongoing WTO plurilateral e-commerce negotiations. Congress may explore the value of digital trade provisions in potential new bilateral trade negotiations.
- Exploring China's digital authoritarianism and its impact on the digital economy and global rules. This could include the effect on U.S. firms doing business in China, as well as the effect on other countries' internet regimes, including identifying which countries or sectors are emulating China's digital rules or technical standards. Congress previously held hearings on the threat to free speech and security aspects posed by PRC internet sovereignty.[100]
- Examining efforts by the United States to counter China's digital policies. For example, investments by the new U.S. International Development Finance Corporation (DFC) could focus on telecommunications and internet infrastructure and policy.[101] Some analysts have suggested that Congress establish a digital development fund dedicated to shaping global norms and developing countries' internet regimes.[102] A bipartisan bill (H.R. 1359) directs executive branch agencies to partner with domestic and foreign partners to "encourage the efforts of developing countries to improve and secure mobile and fixed access to the Internet in order to catalyze innovation, spur economic growth and job creation, … promote free speech, democracy, and good governance… and the multi-stakeholder approach to Internet governance."
- Understanding the potential long-term impact of the splintering internet on the U.S. economy. Without agreement on the underlying rules or convergence on international norms, the risk of a fractured global internet increases. Congressional oversight could examine the value, both economic and political, of U.S. leadership and U.S. norms governing the global internet. Congress could consider asking the U.S. ITC to investigate the economic impact of this fracturing on U.S. businesses and consumers. Congress could

[99] Laurens Cerulus, "EU sounds alarm on foreign interference in 5G networks," *PoliticoPro*, October 9, 2019.

[100] Congressional-Executive Commission on China, *Digital Authoritarianism & The Global Threat to Free Speech*, 116th Cong., April 26, 2018. U.S. Congress, House Permanent Select Committee on Intelligence, *Chinas Digital Authoritarianism: Surveillance, Influence, and Political Control (Open)*, 116th Cong., May 16, 2019.

[101] For more information see, CRS Report R45461, *BUILD Act: Frequently Asked Questions About the New U.S. International Development Finance Corporation*, by Shayerah Ilias Akhtar and Marian L. Lawson.

[102] Daniel Kliman, "Why the United States Needs a Digital Development Fund," Center for a New American Security, October 10, 2019.

- analyze the different approaches and commitments related to internet governance contained in EU or Chinese FTAs, and how they differ from U.S. agreements and objectives. More immediately, Congress could examine the economic impact of the recent technology trade restrictions in China and other countries on U.S. companies.
- Overseeing ongoing efforts to establish global standards and rules through U.S. participation in SDOs, international forums, and recent and ongoing trade negotiations. For example, Congress could hold hearings on U.S. government and private sector involvement in standard-setting and China's increasing role in international standards discussions. Congress could probe executive branch agencies about specific U.S. objectives and engagement in ongoing negotiations related to internet governance and examine if the United States needs a clear strategy for outreach to international partners to build consensus on issues in advance of formal meetings and conferences. Similarly, Congress may consider promoting hosting of some standards meetings and international discussions so that more U.S. stakeholders could participate and provide direct feedback.

Author Information

Rachel F. Fefer
Analyst in International Trade and Finance

Disclaimer