Congressional Research Service
Informing the legislative debate since 1914

Digital Trade and U.S. Trade Policy

Updated December 9, 2021

Congressional Research Service
https://crsreports.congress.gov
R44565

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R44565

December 9, 2021

Rachel F. Fefer, Coordinator
Analyst in International Trade and Finance

Shayerah I. Akhtar
Specialist in International Trade and Finance

Michael D. Sutherland
Analyst in International Trade and Finance

Digital Trade and U.S. Trade Policy

As the global internet expands and evolves, digital trade has become prominent on the global trade and economic policy agenda. According to the Department of Commerce, the "digital economy" accounted for 9.6% of U.S. gross domestic product (GDP) in 2019 and supported 7.7 million U.S. jobs, or 5.0% of total U.S. employment in 2019. From 2005 to 2019, real value added for the U.S. digital economy grew at an average annual rate of 5.2% per year, outpacing the 2.2% growth in the overall economy each year. Digital trade has been growing faster than traditional trade in goods and services, with the pandemic further spurring its expansion.

Congress plays an important role in shaping U.S. policy on digital trade, from oversight of federal agencies charged with regulating cross-border data flows to shaping and considering legislation to implement new trade rules and disciplines through trade negotiations. Congress also works with the executive branch to identify the appropriate balance between digital trasde and other policy objectives, including privacy and national security.

Digital trade includes end-products, such as downloaded movies, and products and services that rely on or facilitate digital trade, such as streaming services and productivity-enhancing tools like cloud data storage and email. In 2020, U.S. exports of information and communications technologies (ICT) services increased to $84 billion, while services exports that could be ICT-enabled totaled $520 billion. Digital trade is growing on a global basis, contributing more to GDP than financial or merchandise flows.

The increase in digital trade raises new challenges in U.S. trade policy, including how to best address new and emerging trade barriers. As with traditional trade barriers, digital trade constraints can be classified as tariff or nontariff barriers. In addition to high tariffs, barriers to digital trade may include localization requirements, cross border data flow limitations, intellectual property rights (IPR) infringement, forced technology transfer, web filtering, economic espionage, and cybercrime exposure or state-directed theft of trade secrets. China's policies, such as those on internet sovereignty and cybersecurity, particularly pose challenges for U.S. companies.

Digital trade issues often overlap and cut across policy areas, such as intellectual property rights (IPR) and national security, raising complex questions for Congress on how to weigh different policy objectives. The Organisation for Economic Co-operation and Development (OECD) points out three potentially conflicting policy goals in the internet economy: (1) enabling the internet; (2) boosting or preserving competition within and outside the internet; and (3) protecting privacy and consumers, more generally.

While no multilateral agreement on digital trade exists in the World Trade Organization (WTO), certain WTO agreements cover some aspects of digital trade. Recent bilateral and plurilateral agreements have begun to address digital trade rules and barriers more explicitly. For example, the U.S.-Mexico-Canada Agreement (USMCA) and ongoing plurilateral discussions in the WTO on an e-commerce agreement could address digital trade barriers to varying degrees. Other international fora also are discussing digital trade, providing the United States with multiple opportunities to engage in and shape global norms.

With workers and firms in the high-tech sector in every U.S. state and congressional district, and with over two-thirds of U.S. jobs requiring digital skills, Congress has an interest in ensuring and developing the global rules and norms of the internet economy in line with U.S. laws and norms, and in establishing a U.S. trade policy on digital trade that advances U.S. national interests

Contents

Introduction 1
Role of Digital Trade in the Economy 2
Economic Impact of Digital Trade 5
COVID-19 and Digital Trade 9
Digitization Challenges 10
Digital Trade Policy and Barriers 12
Tariff and Tax Barriers 13
Nontariff Barriers 15
Localization Requirements 15
Intellectual Property Rights (IPR) Infringement 17
National Standards and Burdensome Conformity Assessment 19
Filtering, Blocking, and Net Neutrality 20
Cybersecurity Risks 21
U.S. Digital Trade with Key Trading Partners 23
European Union 23
General Data Protection Regulation (GDPR) 24
The EU's Digital Policy 25
New EU Copyright Rules 27
U.S.-EU Digital Cooperation 28
China 29
"Cyber Sovereignty" and China's Involvement in Global Internet Governance 31
China's Emerging Cyberspace and Data Protection Regime 32
U.S. Efforts to Address Digital Trade Barriers and IP Theft Issues in China 37
Digital Trade Provisions in Trade Agreements 38
WTO Provisions 39
General Agreement on Trade in Services (GATS) 39
Declaration on Global Electronic Commerce 39
Information Technology Agreement (ITA) 40
Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 40
World Intellectual Property Organization (WIPO) Internet Treaties 41
Current WTO Plurilateral Negotiations 42
U.S. Bilateral and Plurilateral Agreements 43
United States-Mexico-Canada Agreement (USMCA) 44
U.S.-Japan Digital Trade Agreement 45
Other International Forums for Digital Trade 46
Issues for Congress 47

Figures

Figure 1. Digital Economy Value Added by Component 3
Figure 2. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Type of Service 5
Figure 3. Cloud Computing Infrastructure Global Market Share 8
Figure 4. Trans-Atlantic Digitally Enabled Services Trade Flows 24

Tables

Table 1. American Chamber of Commerce in China 2021 Business Survey 30

Contacts

Author Information..... 49

Introduction

The rapid growth of digital technologies in recent years has created new opportunities for U.S. consumers and businesses but also new challenges in international trade. For example, consumers today access e-commerce, social media, telemedicine, and other offerings not imagined thirty years ago. Businesses use advanced technology to reach new markets, track global supply chains, analyze big data, and create new products and services. New technologies facilitate economic activity but also create new trade policy questions and concerns. Data and data flows form a pillar of innovation and economic growth.

The "digital economy" accounted for 9.6% of U.S. gross domestic product (GDP) in 2019, including (1) the information and communications technologies (ICT) sector and underlying infrastructure, (2) business-to-business and business-to-consumer e-commerce, and (3) priced digital services (e.g., internet cloud or intermediary services).[1] The digital economy supported 7.7 U.S. million jobs, or 5.0% of total U.S. employment in 2019.[2] One study found that the "tech-ecommerce ecosystem" added 1.4 million U.S. jobs between September 2017 and September 2021, and was the main job producer in 40 states.[3] As digital information increases in importance in the U.S. economy, issues related to digital trade have become of growing interest to Congress.

While there is no globally accepted definition of digital trade, the U.S. International Trade Commission (USITC) broadly 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).[4]

A joint report by the Organisation for Economic Cooperation and Development (OCED), World Trade Organization (WTO), and International Monetary Fund (IMF) defined digital trade more broadly as "all trade that is digitally ordered and/or digitally delivered."[5]

The rules governing digital trade are evolving as governments across the globe experiment with different approaches and consider diverse policy priorities and objectives. Barriers to digital trade, such as data localization requirements or protectionist industrial policies, often overlap and cut across sectors. In some cases, policymakers may struggle to balance digital trade objectives with other legitimate policy issues, such as national security and privacy. Digital trade policy issues have been in the spotlight recently, due in part to the rise of new trade barriers, heightened concerns over data privacy, the rise of misinformation and disinformation, and an increasing number of cybersecurity incidents that have affected U.S. consumers, companies, and government entities. These concerns may raise the general U.S. interest in managing cross-border data flows, enforcing compliance with existing rules, and establishing new ones. Congress has an

[1] These estimates exclude free digital services. U.S. Bureau of Economic Analysis, *Updated Digital Economy Estimates—June 2021*, June 2021. For more information, see https://www.bea.gov/data/special-topics/digital-economy.

[2] Ibid.

[3] Michael Mandel, "Tech-Ecommerce Drives Job Growth in Most States," Progressive Policy Institute, October 18, 2021, at https://www.progressivepolicy.org/blogs/tech-ecommerce-drives-job-growth-in-most-states/.

[4] U.S. International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, p.33, at https://www.usitc.gov/publications/332/pub4716.pdf.

[5] OECD, WTO, IMF, *Handbook on Measuring Digital Trade*, Version 1, 2020, at http://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf.

interest in ensuring the global rules and norms of the internet economy are in line with U.S. laws and norms and allow for fair global competition for U.S. businesses and workers.

Trade negotiators continue to explore ways to address evolving digital issues in trade agreements, including in the United States' newest agreements, the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement. Congress has an important role in shaping digital trade policy, including overseeing agencies charged with regulating cross-border data flows, as part of trade negotiations, and in working with the executive branch to identify the right balance between digital trade and other policy objectives.

This report discusses the role of digital trade in the U.S. economy, barriers to digital trade, digital trade agreement provisions and negotiations, and other selected policy issues.

Role of Digital Trade in the Economy

The digital economy not only facilitates international trade in goods and services, but is itself a platform for new digitally-originated services. The internet is enabling technological shifts that are transforming businesses. The Group of Twenty (G-20) Digital Economy Task Force identified the digital economy as incorporating "all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services and data. It refers to all producers and consumers, including government, that are utilizing these digital inputs in their economic activities."[6]

The Bureau of Economic Analysis (BEA) estimates that, from 2005 to 2019, real value added for the U.S. digital economy grew at an average annual rate of 5.2% per year, outpacing the 2.2% growth in the overall economy each year.[7] During that time, business-to-consumer e-commerce was the fastest growing component of the digital economy (see **Figure 1**).

The increase in the digital economy and digital trade parallels the growth in internet usage globally. According to one study, over half of the world's population uses the internet.[8] As of 2020, 93% of American adults use the internet, including 15% who only access the internet via smart phones.[9] In the third quarter of 2021, approximately 48% of internet traffic in the United States came from mobile devices.[10] Internet traffic is growing globally, with users making almost

[6] OECD, "A Roadmap Toward a Common Framework for Measuring the Digital Economy for G20 Digital Economy Task Force," Saudi Arabia, 2020, http://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf?utm_source=Adestra&utm_medium=email&utm_content=A%20roadmap%20toward%20a%20common%20framework%20for%20measuring%20the%20Digital%20Economy%20-%20Read%20more&utm_campaign=Stats%20Flash%2C%20August%202020&utm_term=sdd.

[7] U.S. Bureau of Economic Analysis, *Updated Digital Economy Estimates—June 2021*, June 2021. For more information, see https://www.bea.gov/data/special-topics/digital-economy.

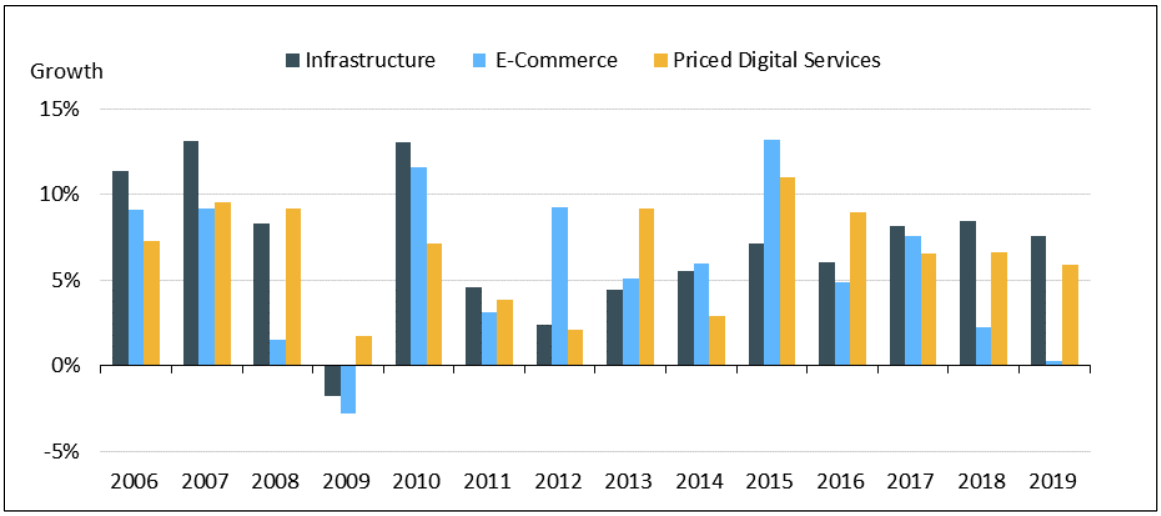
[8] Internet World Stats, *World Internet Usage and Population Statistics*, as of December 31, 2020, at https://internetworldstats.com/stats.htm.

[9] Pew Research Center, *Internet/Broadband Fact Sheet*, April 7, 2021, at https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

[10] Statistica, "Percentage of mobile device website traffic in the United States from 1st quarter 2015 to 2nd quarter 2021," September 30, 2021, at https://www.statista.com/statistics/683082/share-of-website-traffic-coming-from-mobile-devices-usa/.

4.5 million Google searches each minute in 2019.[11] In 2020, the global population is estimated to have generated 47 zettabytes of data—534 million times the internet's size in 1997.[12]

Figure 1. Digital Economy Value Added by Component



Source: U.S. Bureau of Economic Analysis, June 2021.

Cross-border data and communication flows are part of digital trade; they also facilitate trade and the flows of goods, services, people, and finance, which together drive globalization and interconnectedness. The highest levels reportedly are the flows between the United States and Western Europe, Latin America, and China.[13] Efforts to impede cross-border data flows could decrease efficiency and other potential benefits of digital trade.

Powering all these connections and data flows are underlying ICT infrastructure.[14] ICT spending is a large and growing component of the international economy and essential to digital trade and innovation. World trade in ICT physical goods grew to $2.3 trillion in 2020, with U.S. ICT goods exports totaling $138 billion.[15] U.S. exports of ICT goods accounted for 8.7% of total U.S. goods exports in 2019.[16]

Semiconductors, a key component in many electronic devices, including systems that undergird U.S. technological competitiveness and national security, are a top U.S. ICT export. With major semiconductor manufacturing facilities in 18 states, the industry is estimated to employ almost a

[11] Note: Google search is not available in all countries. OECD, "A Roadmap Toward a Common Framework for Measuring the Digital Economy for G20 Digital Economy Task Force," Saudi Arabia, 2020, at https://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf.

[12] A zettabyte is one sextillion (10^{21}) bytes. Digital Economy Compass 2019, Statista.com, at https://www.statista.com/study/52194/digital-economy-compass/.

[13] James Manyika et al., "Digital globalization: The new era of global flows," McKinsey, Global Institute, February 16, 2016.

[14] ICT is an umbrella term that includes any communication device or application, including radio, television, cellular phones, computer and network hardware and software, satellite systems, and associated services and applications.

[15] United Nations Conference on Trade and Development (UNTAC), UNCTADstat, https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=15850.

[16] World Bank, Table: ICT goods exports (% of total goods exports)—United States, https://data.worldbank.org/indicator/TX.VAL.ICTG.ZS.UN?locations=US.

quarter million U.S. workers.[17] The U.S. semiconductor industry dominates many parts of the semiconductor supply chain, such as chip design, and it accounted for 48% (or $193 billion) of the global market of revenue as of 2020.[18] Industry forecasts expect continued strong annual global sales growth of 19.7% in 2021 (to an estimated $527 billion) and a further 8.8% in 2022 (reaching $573 billion).[19] The U.S. share of global semiconductor manufacturing capacity, however, has declined from 37% in 1990 to 12% in 2020.[20] Given the importance of semiconductors to the digital economy and continued advances in innovation, many policymakers see U.S. strength in semiconductor technology and fabrication as vital to U.S. economic and national security interests and have raised concerns about the declining U.S. share in semiconductor manufacturing capacity. Some U.S. policymakers have also expressed concerns about China's state-led efforts to develop an indigenous vertically-integrated semiconductor industry, in part to lessen the country's dependence on U.S. exports.[21]

The growth in traded ICT services is outpacing the growth of traded ICT goods. The OECD estimates that ICT services trade increased 40% from 2010 to 2016.[22] The United States is the third-largest exporter of ICT services, after Ireland and India.[23] ICT services include telecommunications and computer services, as well as charges for the use of intellectual property (e.g., licenses and rights). ICT-enabled services are those services with outputs delivered remotely over ICT networks, such as online banking or education. ICT services can augment the productivity and competitiveness of goods and services. U.S. ICT services are often inputs to final demand products that may be exported by other countries, such as China. U.S. exports of ICT services have grown almost every year since 2000 (see **Figure 2**).[24] In 2020, U.S. exports of ICT services grew to $84 billion of U.S. exports, while exports of potentially ICT-enabled services totaled $520 billion, demonstrating the impact of the internet and digital revolution.[25]

[17] Semiconductor Industry Association, https://www.semiconductors.org/semiconductors-101/industry-impact/.

[18] Semiconductor Industry Association, "Semiconductor Shortage Highlights Need to Strengthen U.S. Chip Manufacturing, Research," February 4, 2021.

[19] Semiconductor Industry Association, "Global Semiconductor Sales Increase 1.9% Month-to-Month in April; Annual Sales Projected to Increase 19.7% in 2021, 8.8% in 2021," June 9, 2021.

[20] Semiconductor Industry Association, "Invest in Domestic Semiconductor Manufacturing and Research," https://www.semiconductors.org/chips/, accessed March 12, 2021.

[21] See CRS Report R46581, *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, by Michaela D. Platzer, John F. Sargent Jr., and Karen M. Sutter, CRS Report R46767, *China's New Semiconductor Policies: Issues for Congress*, by Karen M. Sutter, and Cheng Ting-Fang and Lauly Li, "US-China tech war: Beijing's secret chipmaking champions," *Nikkei Asia*, May 5, 2021.

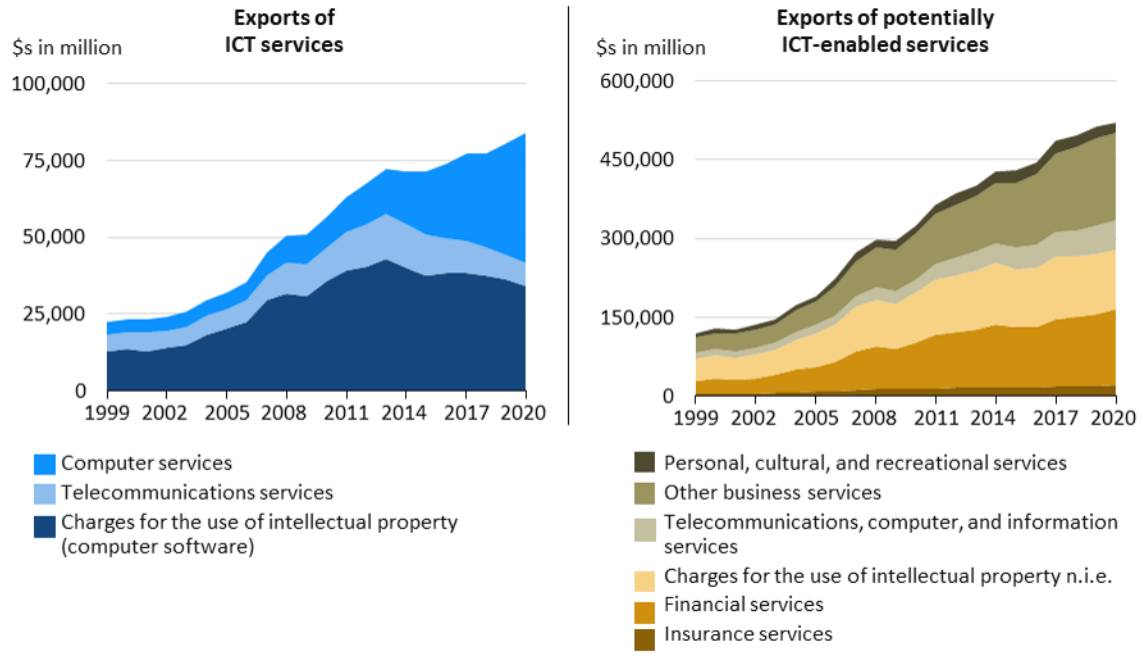
[22] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-en.

[23] Nationmaster, Top Countries in Exports of ICT Services, https://www.nationmaster.com.

[24] Bureau of Economic Analysis, Table 3.1. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Type of Service, June 30, 2020.

[25] According to the Department of Commerce, potentially-ICT enabled services are those that "can predominantly be delivered remotely over ICT networks, a subset of which are actually delivered via that method" and U.S. Bureau of Economic Analysis (BEA), Table 3.1. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Type of Service October 19, 2018.

Figure 2. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Type of Service



Source: U.S. Bureau of Economic Analysis, July 2021.

ICT and other online services depend on software; the value added to U.S. GDP from support services and software has increased over the past decade relative to that of telecommunications and hardware.[26] According to one estimate, software contributed more than $1.9 trillion to the total U.S. value added GDP in 2020 and the software industry accounted for 3.3 million jobs directly in 2020, a 7.2% increase from 2018.[27] According to an industry group, software and the software industry contributes to jobs in all 50 states, with the value-added GDP of the software industry growing more than 35% in Nevada and Washington from 2018 to 2020.[28] The average salary of a software developer is over $114,000.[29] In addition, the software industry claims that the sector funds 27% of all domestic research and development (R&D).[30]

Economic Impact of Digital Trade

As the internet and technology continue to develop rapidly, increasing digitization affects finance and data flows, as well as the movement of goods and people. Beyond simple communication, digital technologies can affect global trade flows in multiple ways and have broad economic impact. First, digital technology enables the creation of new goods and services, such as e-books, online education, or online banking services. Digital technologies may also raise productivity

[26] BEA, *Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts*, March 2018, p.9.

[27] Ibid.

[28] Software.org, "Software: Growing US Jobs and the GDP," https://software.org/wp-content/uploads/2019SoftwareJobs.pdf.

[29] Ibid.

[30] Software.org, *Software: Supporting US Through COVID*, 2021, https://software.org/reports/software-supporting-us-through-covid-2021/.

and/or lower the costs and barriers related to flows of traditional goods and services. For example, some refer to the application of emerging technologies as the Fourth Industrial Revolution (4IR), as companies may rely on radio-frequency identification (RFID) tags and blockchain for global supply chain tracking, 3-D printing based on data files, robotics for manufacturing, or devices or objects connected via the Internet of Things (IoT), and data analytics driven by artificial intelligence (AI) (see **text box** on key technology terms). In addition, digital platforms serve as intermediaries for multiple forms of digital trade, including e-commerce, social media, and cloud computing and allow businesses to reach customers around the globe. In these ways, digitization pervades every industry sector, creating challenges and opportunities for established and new players.

Key Technologies Driving Innovation

Artificial Intelligence (AI) can generally be thought of as computerized systems that work and react in ways commonly thought to require intelligence, such as solving complex problems in real-world situations.

Blockchain is a distributed record-keeping system (each user can keep a copy of the records) that provides for auditable transactions and secures those transactions with encryption. Using blockchain, each transaction is traceable to a user, each set of transactions is verifiable, and the data in the blockchain cannot be edited without each user's knowledge. Compared to traditional technologies, blockchain allows two or more parties without a trusted relationship to engage in reliable transactions without relying on intermediaries or central authority (e.g., a bank or government).

Internet of Things (IoT) is a system of interrelated devices connected to a network and/or to one another, exchanging data without necessarily requiring human-to-machine interaction. In other words, IoT is a collection of electronic devices that can share information among themselves.

Fourth Industrial Revolution (4IR) is characterized by advances in artificial intelligence and machine learning, the Internet of Things, autonomous hardware and software robotics, and advanced data systems that enable real-time and predictive analytics.

Sources: CRS In Focus IF10608, *Overview of Artificial Intelligence*, by Laurie A. Harris; CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer; CRS In Focus IF11239, *The Internet of Things (IoT): An Overview*, by Patricia Moloney Figliola; and COVID-19, 4IR, and the Future of Work, APEC Policy Brief No. 34, June 2020.

In an international context, one source estimates that digitally-enabled trade in 2019 was worth $800 billion to $1.5 trillion (3.5%-6.0% of global trade).[31] Furthermore, up to 70% of all global trade flows could "eventually be meaningfully affected by digitization." One think tank categorizes these trade flows to include digitally-sold trade (e.g., e-commerce), digitally-enhanced trade (e.g., services such as movie streaming or car maintenance monitoring that complement physical goods), and digitally-native trade (e.g., nonfungible token (NFT) or cryptocurrency purchase of digital art or digital platforms).

These estimates do not quantify the additional benefits of digitization for business efficiency and productivity, or of increased customer and market access, which enable greater volumes of international trade in all sectors of the economy. Technology advancements have helped drive efficiency and automation across diverse U.S. industries, but may raise other policy considerations, such as their impact on employment in the manufacturing sector. Digitization efficiencies have the potential to both increase international trade and decrease costs. For example, one analysis found that logistics optimization technologies could reduce shipping and customs processing times by 16% to 28%, boosting overall trade by 6% to 11% by 2030.[32] A

[31] Christian Ketels et al., "Global Trade Goes Digital," Boston Consulting Group, August 12, 2019.

[32] Susan Lund et at., "Globalization in Transition: The Future of Trade and Value Chains," McKinsey & Company, January 2019.

study of small and medium-sized enterprises (SMEs) in Asia found that digital tools reduced export costs by 82%, and transaction times by 29%.[33]

One example of digitization driving efficiencies is the use of AI to help companies forecast demand, understand trends and identify patterns, and allow companies to quickly adjust shipping routes or optimize supply chains when confronted with disruptions or unexpected events.[34] For example, during the COVID-19 pandemic, Samsung noted that "we inserted COVID-specific information, such as closed stores and traffic changes due to the pandemic, into the AI tool to predict the demands more accurately in each region."[35] At the same time, automation, AI, and 3-D printing could enable more local production, thereby reducing global trade by as much as 10% by 2030.[36]

Blockchain is one emerging software technology some companies are using to increase efficiency and transparency and lower supply chain costs that depends on open data flows of digital trade.[37] For example, it is helping services industries, such as insurance, become more efficient by utilizing smart contracts based on blockchain to respond real-time to customers' claims or to streamline fraud mitigation processes.[38] Another example is how, in an effort to streamline processes, save costs, and improve public health outcomes, Walmart and IBM built a blockchain platform to increase transparency of global supply chains and improve traceability for certain imported food products.[39] The initiative aims to expand to include several multinational food suppliers, farmers, and retailers and depends on connections via the IoT and open international data flows.

According to one global estimate, there are 26 billion internet-connected vehicles, industrial equipment and household items that could transmit data for companies and government to analyze to improve processes and outcomes, whether efficiency or consumer welfare.[40] Software drives these connected products, merging the physical and digital world and facilitating the delivery of new global services embedded in products. The overall and long-term impact of digitization has yet to be seen. One think tank estimates that 60% of global GDP will be digitized by 2022, with growth in every industry driven by data flows and digital technology.[41]

Because of its ubiquity, the benefits and economic impact of digitization are not restricted to certain geographic areas, and businesses and communities in every U.S. state feel the impact of digitization, as new business models and jobs are created and existing ones are disrupted.[42] For

[33] AlphaBeta, "Micro-Revolution: The New Stakeholders of Trade in APAC," Asia Pacific MSME Trade Coalition, February 2018.

[34] James Rundle, "Supply Chain Strains Sharpen Focus on AI," *The Wall Street Journal*, March 31, 2021.

[35] Edward White, "Companies try to cut geopolitical risk from supply chains," *The Financial Times*, April 6, 2021.

[36] Ibid.

[37] For more on blockchain, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

[38] Adelyn Zhou, "How Blockchain Smart Contracts Are Reinventing the Insurance Industry," *Nasdaq*, January 29, 2021, and Gemini, "Blockchain and the Insurance Industry," Cryptopedia, March 24, 2021.

[39] Walmart, "Food Traceability Initiative Fresh Leafy Greens," letter to suppliers, September 24, 2018, https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/_proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001.

[40] Hosuk Lee-Makiyama and Kimberley Botwright, "5 ways to ensure trust when moving data across borders," World Economic Forum, April 13, 2021.

[41] Frank Gens et al., "IDC FutureScape: Worldwide IT Industry 2019 Predictions," October 2018.

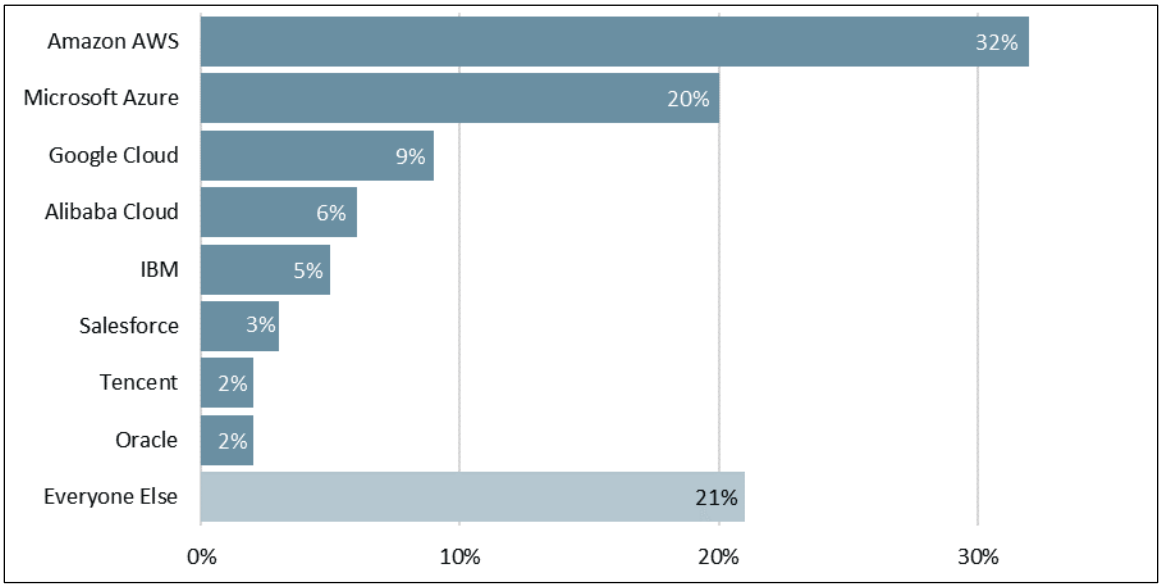
[42] John Wu, Adams Nager, and Joseph Chuzhin, *High-Tech Nation: How Technological Innovation Shapes America's 435 Congressional Districts*, ITIF, November 28, 2016, p. 4, https://itif.org/publications/2016/11/28/technation.

example, a small business that uses accounting software may no longer need to employ a bookkeeper, while a neighborhood store may confront new competition from online sellers based in other countries, but also develop its own online sales channel. One study found that the more intensively a company uses the internet, the greater the productivity gain. The increase in internet usage is also associated with increased value and diversity of products being sold.[43]

One driver of the diffusion of the benefits of the internet and digitization has been cloud computing. Cloud services have been called the great equalizer, since they generally allow small companies access to the same information and the same computing power as large firms using a flexible, scalable, and on-demand model. In 2020, the global cloud computing market was estimated to be worth $130 billion annually—dominated by U.S. and Chinese firms, with Amazon Web Services (AWS) as the world's largest supplier (see **Figure 3**).[44]

Figure 3. Cloud Computing Infrastructure Global Market Share

As of end 2020



Source: Synergy Research Group, "Cloud Market Ends 2020 on a High while Microsoft Continues to Gain Ground on Amazon," February 2, 2021.

Digital platforms can minimize costs and enable SMEs to grow through extended reach to customers or suppliers or by integrating into global value chains (GVCs). For example, Amazon notes that hundreds of thousands of SMEs launch and scale their businesses using AWS and that SMEs selling on Amazon.com have created an estimated 1.1 million jobs.[45] Netflix, a U.S. firm offering online streaming services, earned more revenue from international markets than from the U.S. domestic market in the first quarter of 2021.[46]

[43] The World Bank Group, *World Development Report 2016: Digital Dividends*, 2016, http://www.worldbank.org/en/publication/wdr2016.

[44] Synergy Research Group, "Race for the Cloud," *Politico*, April 22, 2021.

[45] Amazon, *2020 Amazon SMB Impact Report*, https://assets.aboutamazon.com/4d/8a/3831c73e4cf484def7a5a8e0d684/amazon-2020-smb-report.pdf.

[46] Netflix, Streaming Revenue and Membership Information by Region, Netflix First Quarter 2021 Earnings Interview, https://ir.netflix.net/ir-overview/profile/default.aspx.

Digitization of customs and border control mechanisms also may help simplify and speed delivery of goods to customers. Regulators are looking to blockchain technology to improve efficiency in managing and sharing data for functions such as border control and customs processing of international shipments.[47] With simpler border and customs processes, more firms are able to conduct business in global markets (or are more willing to do so). A study of U.S. SMEs on the e-commerce platform eBay found that 96% export to an average of 17 foreign countries.[48] Digital trade facilitation (e.g., digitizing customs, legal documents, and supply chain finance) has gained prominence on the international trade agenda, as policymakers and businesses seek to enable export opportunities for SMEs.

A similar argument has been made for firms and governments in low- and middle-income countries who can take advantage of the power of the internet to foster economic development. In the Asia-Pacific Economic Cooperation (APEC) region, which includes the United States, for example, SMEs account for over 97% of all business and employ over half of the workforce.[49] Recognizing the importance of digitization, APEC officials agreed to focus on initiatives to develop the digital potential of Micro, Small and Medium Enterprises (MSMEs), including women-owned businesses.[50] A 2011 study of SMEs estimated that the internet is a net creator of jobs, with 2.6 jobs created for every job that may be displaced by internet technologies; companies that use the internet intensively effectively doubled the average number of jobs.[51] As technology has evolved since 2011, the job impact may be greater today, but the benefits and costs of digitization and digital trade can vary across sectors.

COVID-19 and Digital Trade

When the COVID-19 pandemic began in early 2020, services trade declined across the globe, with tourism (the top U.S. cross-border services export), transport, and distribution impacted the most.[52] Despite the overall decline, digital trade in services, including online retail, health, education, audio-visual services, and telecommunications, saw some significant gains as consumers and workers stayed home. The WTO noted the global shift to digital services, stating that "consumers are adopting new habits that may contribute to a long-term shift towards online services."[53] Governments have helped enable the transition through new permanent and temporary measures, such as allowing for medical consultations online, demonstrating the importance of digital trade.[54] Software and digital connections also allowed the shift to telework

[47] Commercial Customs Operations Advisory Committee (COAC), *Trade Progress Report*, November 2017, https://www.cbp.gov/sites/default/files/assets/documents/2017-Nov/Global%20Supply%20Chain%20Subcommittee%20Trade%20Executive%20Summary%20Nov%202017.pdf.

[48] Cathy Foster, "eBay's 2020 U.S. Small Online Business Report: How We're Creating Economic Opportunity," July 16, 2020, https://www.ebayinc.com/stories/news/ebays-2020-u-s-small-online-business-report-how-were-creating-economic-opportunity/.

[49] Https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Small-and-Medium-Enterprises.

[50] 2020 APEC SME Ministerial Statement, "Navigating the New Normal: Restarting and Reviving MSMEs through Digitalisation, Innovation and Technology, October 23, 2020.

[51] Matthieu Pélissié du Rausas, James Manyika, and Eric Hazan et al., *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*, McKinsey Global Institute, May 2011, p. 21, http://www.mckinsey.com/industries/high-tech/our-insights/internet-matters.

[52] WTO, "Trade in Services in the Context of COVID-19," May 28, 2020.

[53] Ibid.

[54] For more information and examples see, WTO, COVID-19: Measures affecting trade in services, https://www.wto.org/english/tratop_e/covid19_e/trade_related_services_measure_e.htm.

(or remote work) for many employees accustomed to working in a busy office or traveling domestically or abroad to meet customers or suppliers in person. However, gains from digitization did not fully compensate for the decline in trade as the WTO noted that total global trade in services was down by a 21% in 2020, compared to 2019.[55]

Just as the COVID-19 pandemic accelerated the shift to online provision of services, it also pushed companies to adopt new Fourth Industrial Revolution (4IR) technologies, such as robotics and automation. According to one study, 40% of companies worldwide are increasing their use of automation as a response to the pandemic and restrictions, such as social distancing guidelines.[56] For example, one grocery chain in the Netherlands is developing robotics and AI for use in store operations to place and remove products.[57]

The growth in online services and automation created increased demand for the ICT goods that enable such shifts (e.g., laptops for e-learning and telework), leading to a surge in semiconductor demand, which outstripped supply.[58] Auto plants in particular were hit hard, after the industry initially lowered their purchases of semiconductors during initial pandemic lockdowns, reflecting lower customer demand for autos. When demand began to grow as countries opened up, automakers around the world found themselves without needed components, leading many to decrease or stop auto production altogether.[59] Many U.S. policymakers and other observers have called for increased investment in semiconductor manufacturing to power the shift online and to further digital advancements.[60]

The pandemic further underscored ongoing digital challenges in the United States and across the world. For example, mitigation efforts, such as the switch to online shopping, education, and telemedicine, revealed discrepancies in broadband availability and accessibility—termed the digital divide—across the United States.[61]

Digitization Challenges

The importance of digitization to the U.S. economy is expected to grow. Many in business and research communities are only beginning to understand how to take advantage of the vast amounts of data being collected every day, one important aspect of the digital economy. One study estimates companies are using 32% of data available to them to create value.[62]

---

[55] WTO, "Services trade slump persists as travel wanes; other service sectors post diverse gains," July 23, 2021.

[56] Angus Loten, "Tech Workers Fear Their Jobs Will Be Automated in Wake of Coronavirus," *The Wall Street Journal*, May 27, 2020.

[57] Catherine Stupp, "Ahold Delhaize Accelerates Automation as Coronavirus Pressures Workforce," *The Wall Street Journal Pro*, May 15, 2020.

[58] Falan Yinug, "Semiconductor Shortage Highlights Need to Strengthen U.S. Chip Manufacturing, Research," Semiconductor Industry Association, February 4, 2021.

[59] Mike Colias, "GM to Halt Production at Several North American Plants Due to Chip Shortage," *The Wall Street Journal*, April 8, 2021. For more information on semiconductors, see CRS Report R46581, *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, by Michaela D. Platzer, John F. Sargent Jr., and Karen M. Sutter.

[60] See CRS Report R46581, *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, by Michaela D. Platzer, John F. Sargent Jr., and Karen M. Sutter.

[61] For more information on the U.S. digital divide and COVID-19, see CRS Insight IN11239, *COVID-19 and Broadband: Potential Implications for the Digital Divide*, by Colby Leigh Rachfal.

[62] Seagate, "Rethink Data: Put More of Your Business Data to Work—From Edge to Cloud," July 2020, https://www.seagate.com/files/www-content/our-story/rethink-data/files/Rethink_Data_Report_2020.pdf.

While new technologies and new business models present opportunities to enhance efficiency and expand revenues, innovate faster, develop new markets, and achieve other benefits, new challenges also arise with the disruption of supply chains, labor markets, and some industries. A 2020 study found that, in the United States and United Kingdom, almost 20% of jobs are in ICT-intensive occupations, highlighting the importance of a digitally-skilled workforce.[63] Another found a mismatch between workforce skills and job openings—67% of new U.S. science, technology, engineering, and mathematics (STEM) jobs are in computing whereas 11% of STEM degrees are in computer science.[64]

With the rapid pace of technology innovation, more jobs may become automated, with digital skills becoming a foundation for economic growth for individual workers, companies, and national GDP.[65] An OECD survey found that most countries, except the United States, have federal policies to promote the use of digital technologies by businesses.[66] A separate OECD study found that, in general, SMEs tend to lag in some areas of digitization.[67] The report includes policy recommendations, such as government investments in awareness campaigns and technology training, as well as the development of SME-tailored digital solutions. [68]

The World Bank identified policy areas to try to ensure, and maintain, the potential benefits of the digital economy.[69] These policy areas include establishing a favorable and competitive business climate, developing strong human capital, ensuring good governance, investing to improve both physical and digital infrastructure, and raising digital literacy skills. Some countries have established national digital strategies (NDSs) to help governments shape the way digital transformation takes place in a country that define policy priorities, set objectives and outline actions for implementation.[70] Although the United States lacks an overarching digital strategy, according to the World Economic Forum's 2020 Global Competitiveness Report, the United States is ranked number one for "digital legal framework" (the U.S. legal framework is able to adapt to digital business models), but it is not in the top ten countries for "digital skills" (a high percentage of the U.S. workforce may not be able to adapt to digitization due to a lack of digital skills).[71]

[63] OECD, "A Roadmap Toward a Common Framework for Measuring the Digital Economy for G20 Digital Economy Task Force," Saudi Arabia, 2020, https://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf.

[64] STEM stands for Science, technology, engineering, and mathematics. Computer Science Education Stats, https://code.org/promote.

[65] The World Bank Group, *World Development Report 2016: Digital Dividends*, 2016, http://www.worldbank.org/en/publication/wdr2016.

[66] OECD (2020), OECD Digital Economy Outlook 2020, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en.

[67] OECD (2021), *The Digital Transformation of SMEs*, OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, https://doi.org/10.1787/bdb9256a-en.

[68] Ibid.

[69] The World Bank Group, *World Development Report 2016: Digital Dividends*, 2016, http://www.worldbank.org/en/publication/wdr2016.

[70] OECD (2020), OECD Digital Economy Outlook 2020, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en.

[71] World Economic Forum, *Global Competitiveness Report Special Edition 2020: How Countries are Performing on the Road to Recovery*, December 16, 2020.

Digital Trade Policy and Barriers

Policies that affect digitization in any one country's economy can have consequences beyond its borders. Because the internet is a global "network of networks," the state of a country's digital economy also can have global ramifications. Protectionist policies may erect barriers and create discriminatory practices to digital trade, or damage trust in the underlying digital economy, and can result in the fracturing, or so-called balkanization, of the internet, lessening any economic gains.[72] What some policymakers see as protectionist, however, others may view as necessary to protect domestic interests.

Despite common core principles, such as protecting citizens' privacy and expanding economic growth, many governments face multiple challenges in designing policies around digital trade. The OECD points out three potentially conflicting policy goals in the digital economy: (1) enabling the internet; (2) boosting or preserving competition within and outside the internet; and (3) protecting privacy and consumers more generally.[73]

Ensuring the free flow of information and open internet and defending freedom of online expression are longstanding U.S. policy priorities.[74] Like other cross-cutting policy areas, such as cybersecurity or privacy, no one federal entity has policy primacy in every area of digital trade, and the United States has taken a sectoral approach to regulating digitization. According to an OECD study, the United States is the only OECD country that uses a decentralized, market-driven approach for a digital strategy, rather than having an overarching national digital strategy, agenda, or program.[75]

The executive branch advocates for U.S. digital priorities and noted many of them, such as working with allies to counter digital authoritarianism and establish international rules for emerging technologies, in its National Security Strategy report.[76] Federal agencies identify and challenge foreign trade barriers through trade negotiations. The Department of Commerce works to promote U.S. digital trade policies domestically and abroad. Commerce's digital attaché program under its foreign commercial service helps U.S. businesses navigate regulatory issues and overcome trade barriers to e-commerce exports in key markets.[77]

The U.S. Trade Representative (USTR), a Cabinet-level official in the Executive Office of the President, is the President's principal advisor on trade policy, chief U.S. trade negotiator, and head of the interagency trade policy coordinating process. In describing the Biden Administration's worker-centric digital trade policy, USTR Katherine Tai stated that "our efforts to formulate and pursue digital trade policies should, therefore, begin with a high level of ambition to be holistic and inclusive," and that "digital trade policy must be grounded in how it affects our people and our workers."[78] She explained that in defining the Administration's digital

[72] For example see, A. Michael Spence, "Preventing the Balkanization of the Internet," Council on Foreign Relations, March 28, 2018, or Keith Wright, "The 'splinternet' is already here," *TechCrunch*, March 3, 2019.

[73] Koske, I. et al. (2014), "The Internet Economy—Regulatory Challenges and Practices," OECD Economics Department Working Papers, No. 1171, OECD Publishing, Paris. DOI, http://dx.doi.org/10.1787/5jxszm7x2qmr-en.

[74] Https://www.state.gov/world-press-freedom-day/.

[75] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, p. 34, http://dx.doi.org/10.1787/9789264276284-en.

[76] The White House, *Interim National Security Strategic Guidance*, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[77] For more information, see https://www.export.gov/digital-attache.

[78] U.S. Trade Representative, *Remarks of Ambassador Katherine Tai on Digital Trade at the Georgetown University*

trade policy, USTR is asking "big and consequential questions," including on the linkage with national security, domestic, and foreign policy interests; how best to work with allies; and how to balance the right of governments to regulate with the need for international trade rules.[79]

In passing Trade Promotion Authority (TPA) in 2015, Congress set negotiating objectives for USTR to pursue in trade negotiations, including related to digital trade (see **text box**).

2015 U.S. Digital Trade Negotiating Objectives

Congress enhanced its 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. TPA 2015 objectives related to digital trade directed the Administration to negotiate agreements that

- ensure application of existing WTO commitments to the digital trade environment, ensuring no less favorable treatment to physical trade;
- prohibit forced localization requirements and restrictions to digital trade and data flows;
- keep electronic transmissions duty-free; and
- ensure relevant legitimate regulations are as least trade restrictive as possible.

Other negotiating objectives in TPA had implications for digital trade. For instance, objectives related to intellectual property rights (IPR) included ensuring that "rightsholders have the legal and technological means to control the use of their works through the Internet and other global communications media, and to prevent the unauthorized use of their works" and "providing strong protection for new and emerging technologies and new methods of transmitting and distributing products embodying intellectual property, including in a manner that facilitates legitimate digital trade."

TPA expired on July 1, 2021. Should Congress consider new TPA legislation, an issue that it may confront is whether to expand or amend the digital trade negotiating priorities.

See CRS In Focus IF10038, *Trade Promotion Authority (TPA)*, by Ian F. Fergusson, and CRS Report RL33743, *Trade Promotion Authority (TPA) and the Role of Congress in Trade Policy*, by Ian F. Fergusson.

As with traditional trade barriers, digital trade constraints can be classified as tariff or nontariff barriers. Tariff barriers may increase the cost of imported goods used to create ICT infrastructure that make digital trade possible or on the products that allow users to connect, while nontariff barriers, such as discriminatory regulations or local content rules, can block or limit different aspects of digital trade. Such barriers may be intended to shield domestic producers and suppliers, safeguard national security, or protect consumer safety.

Tariff and Tax Barriers

Historically, trade policymakers focused on addressing overt trade barriers, such as tariffs or quotas for imported products. Tariffs at the border impact goods trade by raising the prices of products for producers or end customers, if tariff costs are passed down, thus limiting market access for U.S. exporters selling products, including ICT goods. Quotas may limit the number or value of foreign goods, persons, suppliers, or investments allowed in a market. Since 1998, WTO countries have agreed to not impose customs duties on electronic transmissions covering both goods (such as e-books and music downloads) and services.[80] Whether the moratorium will be continued after its current expiration after the upcoming Ministerial meeting or made permanent is subject to debate in the WTO (see "Declaration on Global Electronic Commerce" below).

Law Center Virtual Conference, November 3, 2021.

[79] Ibid.

[80] *The Geneva Ministerial Declaration on global electronic commerce*, WT/MIN(98)/DEC/2, May 25, 1998.

While the United States is a major exporter and importer of ICT goods, tariffs are not levied on many of the products due to commitments in U.S. free trade agreements (FTAs) and the WTO Information Technology Agreement (ITA). Tariffs may serve as trade barriers for those countries or products not covered by existing FTAs or the WTO ITA.

Digital Tariff and Tax Barriers: Selected Examples

- An Indonesian regulation placed software and other digital products transmitted electronically, including applications, software, video, and audio, on its tariff schedule. Although the tariffs are currently set to zero, U.S. companies are raising concerns about potential tariffs and administrative burdens, including customs documentation.[81]
- In Bangladesh, foreign satellite television service and social media suppliers must pay a 15% VAT and open local offices or appoint local representatives to facilitate tax collection.
- The Mexican government has the power to order local Internet Service Providers (ISPs) to block access to electronically delivered services from foreign service suppliers who do not comply with Mexican VAT rules.

Source: U.S. Trade Representative, 2021 National Trade Estimate Report on Foreign Trade Barriers, March 31, 2021, p. 282, https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf.

More recently, noting the growth of the digital economy, some countries, particularly in Europe and Asia, have proposed, announced, or implemented unilateral digital services taxes (DSTs) on the gross revenues earned by multinational corporations (MNCs) active in the digital economy. For example, France enacted a DST that applies a 3% levy on gross revenues derived from two digital activities of which French "users" are deemed to play a major role in value creation. Some countries have argued that such DSTs can serve as a market access barriers. USTR concluded that France's DST discriminates against major U.S. digital companies and is inconsistent with prevailing international tax policy principles.[82]

In June 2021, the United States and more than 130 countries agreed to update the global tax system and develop an international digital tax framework at the OECD. In support of the G-20/OECD Inclusive Framework negotiations, in June 2021, the United States and other G-7 countries announced agreement on (1) how to allocate taxing rights of the largest and most profitable multinational enterprises, including digital companies, and (2) a global minimum tax.[83] In October, the United States reached a compromise—the "Agreement on DSTs"—with several European countries to withdraw their national DSTs once the multilateral deal goes into effect and to credit companies with any excess taxes paid. As part of it, the United States agreed to terminate the currently-suspended Section 301 trade actions against Austria, France Italy, Spain, and the UK.[84] The United States reached a similar agreements with Turkey and India in

[81] U.S. Trade Representative, *2021 National Trade Estimate Report on Foreign Trade Barriers*, March 31, 2021, p. 282, https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdft.

[82] For more information on the USTR investigations, see CRS In Focus IF11564, *Section 301 Investigations: Foreign Digital Services Taxes (DSTs)*, by Andres B. Schwarzenberg.

[83] U.S. Department of the Treasury, *G7 Finance Ministers & Central Bank Governors Communique*, Press release, June 5, 2021, https://home.treasury.gov/news/press-releases/jy0215; OECD, *Statement on a Two-Pillar Solution to Address the Tax Challenges Arising From the Digitalisation of the Economy*, July 1, 2021, https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-july-2021.htm. For more information on the international tax negotiations, see CRS In Focus IF11874, *International Tax Proposals Addressing Profit Shifting: Pillars 1 and 2*, by Jane G. Gravelle.

[84] For more details on the compromise, see U.S. Department of the Treasury, *Joint Statement from the United States, Austria, France, Italy, Spain, and the United Kingdom, Regarding a Compromise on a Transitional Approach to Existing Unilateral Measures During the Interim Period Before Pillar 1 is in Effect*, October 21, 2021, and USTR, *USTR Announces, and Immediately Suspends, Tariffs in Section 301 Digital Services Taxes Investigations*, Press release, June 2, 2021.

November.[85] The USTR, in coordination with the U.S. Department of the Treasury, is to monitor the implementation of the agreement.

Digital Trade Restrictiveness Index (DSTRI)

The OECD Services Trade Restrictiveness Index (STRI) provides information on regulations affecting trade in services across a set of countries and 22 sectors that represent over 80% of global trade in services. A subset of the STRI measures the regulatory environment for digitally-enabled services (Digital STRI or DSTRI). For the 2020 DSTRI, Kazakhstan was the most restrictive country, outranking China, while Canada and Costa Rica were the least restrictive. The United States was in third place for least restrictive, tied with Australia, Estonia, Luxembourg, Switzerland, and the United Kingdom. U.S. barriers included restrictions on electronic transactions reflecting some U.S. sector-specific rules.

Source: OECD, Services Trade Restrictiveness Index, https://stats.oecd.org/Index.aspx?DataSetCode=STRI#.

Nontariff Barriers

Nontariff barriers (NTBs) are not as easily quantifiable or identifiable as tariffs. Like digital trade, NTBs to digital trade have evolved and may pose significant hurdles to companies seeking to do business abroad. NTBs often called "behind the border" trade barriers come in the form of laws or regulations that intentionally or unintentionally discriminate against and/or hamper the free flow of digital trade.

Potential Barriers to Digital Trade

- High tariffs or low quotas
- Localization requirements
- Cross border data flow limitations
- Intellectual property rights (IPR) infringement
- Discriminatory, unique technical standards or burdensome testing and certification requirements
- Filtering or blocking
- Restrictions on electronic payment systems or the use of encryption
- Cybertheft of U.S. trade secrets
- Forced technology transfer

Nondiscrimination between local and foreign suppliers is a core principle encompassed in global trading rules and U.S. FTAs. While WTO agreements cover physical goods, services, and intellectual property, there is no explicit provision for nondiscrimination for digital goods. As such, NTBs that do not treat digital goods the same as physical ones could limit a provider's ability to enter a market.

Broader governance issues, including rule of law, transparency, and investor protections, can pose barriers and limit the ability of firms and individuals to engage in digital trade. Similarly, market access restrictions on investment and foreign ownership, or on the movement of people, whether or not specific to digital trade or ICT sectors, may limit a company's ability to enter a foreign market. Other NTBs are more specific to digital trade.

Localization Requirements

Localization measures are defined as measures that compel companies to conduct certain digital-trade-related activities within a country's borders.[86] Governments often use privacy protection or national security arguments as justifications for these measures. Though some localization policies may be used to achieve legitimate public policy objectives, including national security or

[85] U.S. Trade Representative, *USTR Welcomes Agreement with Turkey on Digital Services Taxes*, November 22, 2021, and *USTR Welcomes Agreement with India on Digital Services Taxes*, November 24, 2021.

[86] U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1*, Publication No: 4415, Investigation No: 332-531, July 2013, p. 16, https://www.usitc.gov/publications/332/pub4415.pdf.

personal data protection, some are designed to protect, favor, or stimulate domestic industries, service providers, or intellectual property at the expense of foreign counterparts and, in doing so, function as NTBs to market access. In recent FTAs, the United States has aimed to ensure an open internet and eliminate digital trade barriers, while preserving flexibility for governments to pursue legitimate policy objectives (see below).

Cross-Border Data Flow Restrictions

According to a 2017 USITC report, businesses most frequently cite data localization as impeding digital trade. A separate study found that, as of 2019, there were over 200 data regulations globally, including those relating to data transfers and local storage requirements.[87] Regulations limiting cross-border data flows and requiring local storage are a type of localization requirement that prohibit companies from exporting data outside a country.

Such restrictions can pose barriers to companies whose transactions rely on the internet to serve customers abroad and operate more efficiently. For example, data localization requirements can limit e-commerce transactions that depend on foreign financial service providers or multinational firms' full analysis of big data from across an entire company or global value chain. Many of the emerging technologies driving innovation and business productivity gains, such as blockchain for supply chain tracking or IoT for maintenance monitoring, rely on cross-border data flows. One study in three developing regions found that data localization measures on IoT applications and related data could cut 59%-68% of a region's productivity and revenue gains and result in job losses by raising data storage costs, forcing companies to use potentially lower quality local vendors, and deterring investment.[88] Furthermore, regulations limiting cross-border data flows may force companies to build local server infrastructure within a country, not only increasing costs and decreasing scale, but also creating data silos that may be more vulnerable to cybersecurity risks. According to some analysts, computing costs in markets with localization measures can be 30%-60% higher than in more open markets.[89]

Data localization requirements pose barriers to companies' efforts to operate more efficiently by migrating to the cloud or SMEs' attempts to enter new markets. These trade barriers may be of specific concern to U.S. trade policy, given that most of the largest global providers of cloud computing services are U.S. companies (specifically Amazon, Microsoft, Google, and IBM). Regulations or policies that limit data flows create barriers to firms and countries seeking to consume cloud services. Finding a global consensus on how to balance reciprocal and open data flows, cybersecurity, and privacy protection may be key to maintaining trust in the digital environment and advancing international trade.[90] Countries are debating how to achieve the right balance and potential paths forward in plurilateral and multilateral forums and trade negotiations (see "U.S. Bilateral and Plurilateral Agreements").

---

[87] U.S. International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017, https://www.usitc.gov/publications/332/pub4716.pdf, and David Nguyen and Marta Paczos, "Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective," OECD Digital Economy Papers No. 297, August 2020.

[88] Hosuk Lee-Makiyama and Simon Lacey, "Cross-Border Data Flows: The impact of data localisation on IoT," GSMA, January 2021.

[89] David J. Lynch, "The U.S. dominates the world of big data. But Trump's NAFTA demands could put that at risk," *Washington Post*, November 28, 2018.

[90] For more information on data flows, see CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

Other Localization Requirements

In addition to cross-border data flow restrictions, localization policies include requirements to use local content, whether hardware or software, as a condition for manufacturing or access to government procurement contracts; use local infrastructure or computing facilities; or partner with a local company and transfer technology or intellectual property to that partner. Localization requirements can also pose a threat to intellectual property (discussed below).

Examples of Localization Barriers

Examples of localization barriers include the following:

- Russia requires that certain data collected electronically by companies on Russian citizens be processed and stored in Russia and that some communications content be stored locally for six months, with related metadata stored for even longer periods of time.
- South Korea maintains localization requirements for payment gateway services' data storage facilities.
- The Reserve Bank of India mandates payment service suppliers to store all information related to electronic payments by Indian citizens on servers located in India. India is also considering a new electronic commerce policy which could include data localization requirements and restrictions on cross-border data flows.
- China passed a nationwide Data Security Law that, among other requirements, mandates that firms store all data generated by Chinese firms and customers in China in accordance with a domestic "secure and controllable" data security standard.

Sources: 2021 National Trade Estimate Report on Foreign Trade Barriers, Office of the United States Trade Representative, March 2021; Stanford DigiChina Cyber Policy Center, "Translation: Data Security Law of the People's Republic of China," June 29, 2021.

Intellectual Property Rights (IPR) Infringement

Many digital companies seek to protect their works through IPR—legal rights that governments grant to inventors and artists to exclude others from using their creations without their permission, usually for a certain period of time. IPR regimes aim to incentivize innovation, while also encouraging dissemination of the outcomes of those innovative activities, though the balance among these goals is subject to policy debate.[91]

Copyright is a key form of protection for creative content licensed and distributed online. While patents remain a dominant form of protection for technological inventions, trade secrets also are becoming more prevalent and valuable in the digital economy.[92] Other forms of IPR include trademarks, such as for brand names and domain names. IPR is also a type of digital trade as it can be sold or licensed.

While the internet and digital technologies have opened up new markets for international trade, they also present ongoing and unique challenges for protecting and enforcing IPR. Digital innovations, for instance, can enable the rapid duplication and distribution of content that is low-cost and high-quality, making it easy, for instance, to pirate music, movies, software, and other copyrighted works, and to share them globally. Another illustration is trade secrets, which are increasingly vulnerable to theft "because they are stored and communicated in digital networks,

[91] See CRS Report RL34292, *Intellectual Property Rights and International Trade*, by Shayerah I. Akhtar, Ian F. Fergusson, and Liana Wong.

[92] Robert D. Atkinson, "IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues," ITIF, January 2019. In some cases, patents and trademarks may be complementary, with patents protecting the primary invention and trade secrets protecting the related "know-how."

with hundreds or thousands of devices in the hands of users; and in part because globalization requires sharing sensitive data with development partners and across distant supply chains."[93]

USITC has identified the infringement of IPR associated with digital products or services as digital trade barriers. USITC has noted that poor IPR protection in a country's legal framework or the weak enforcement of such IPR can lead to extensive digital piracy, which can potentially limit "the profitability and commercial viability of digital content providers."[94] USTR identifies specific concerns about digital piracy in its latest annual "Special 301" review of foreign countries' IPR regimes (see **text box**).[95] Increased use of digital services and related demand shifts during the COVID-19 pandemic have stressed IPR regimes and exacerbated IPR infringement concerns.[96]

Examples of IPR Issues in the Digital Environment

The Office of the U.S. Trade Representative (USTR) identified online piracy as the most challenging copyright enforcement issue in many countries, including those in the "Priority Watch List" such as Argentina, Chile, China, India, Russia, and Ukraine. These concerns include

- stream-ripping (the unauthorized conversion of a file from a licensed stream site into an unauthorized copy), commonly to pirate music;
- online distribution of software and devices that allow for the circumvention of technological protection measures (TPMs) used to control manage access to copyrighted works;
- the use of illicit streaming devices (ISDs) and illicit Internet Protocol Television (IPTV) service apps to access live sporting events and performances and other copyrighted content; and
- the use of unlicensed software by foreign governments, which also raises concerns about malware.

Other concerns identified by USTR include

- illegal camcording of movies in theater, which drives unauthorized copies of newly released movies online;
- "cybersquatting," the unauthorized domain name registration and trademark uses in some country code top-level domain names (ccTLDs), which can cause right holders to incur loss of valuable internet traffic; and
- cybertheft of trade secrets and gaps in trade secret protection in countries such as China, Russia, and India.

Sources: USTR, 2021 Special 301 Report, April 2021; and USTR, 2020 Review of Notorious Markets for Counterfeiting and Piracy, January 2021.

The losses from IPR infringement in the digital environment are considered to be significant, but difficult to quantify and depend on various assumptions, including the extent to which IPR infringement actually displaces legal sales.[97] In 2017, the Commission on the Theft of American Intellectual Property estimated that the value of the annual cost to the U.S. economy from three major categories of IP theft surpasses $225 billion and could be as high as $600 billion. The three categories were: counterfeit and pirated tangible, traded goods (low-end estimate of $29 billion, high-end of $41 billion); pirated U.S. software (estimated value of $18 billion); and trade secret theft (low-end estimate of $180 billion, high-end estimate of $540 billion).[98] A 2018 report by

[93] International Chamber of Commerce (ICC), *The ICC Intellectual Property Roadmap*, 2020, p. 74.

[94] USITC, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, p. 17.

[95] See U.S. Trade Representative, *2021 Special 301 Report*, April 2021.

[96] USITC, *Recent Trends in U.S. Services Trade: 2021 Annual Report*, p. 104.

[97] Brett Danaher, Michael D. Smith, and Rahul Telang, "Piracy Landscape Study: Analysis of Existing and Emerging Research to Intellectual Property Rights (IPR) Enforcement of Commercial-Scale Piracy," USPTO, USPTO Economic Working Paper Series, April 2020.

[98] These estimates do not include patent infringement. Commission on the Theft of American Intellectual Property ("IP Commission," which characterizes itself as an independent, bipartisan initiative of members from the public and private sector), *The Theft of American Intellectual Property: Reassessments of the Challenge and U.S. Policy—Update to the*

McAfee and the Center for Strategic and International Studies (CSIS) estimated annual losses from cyber theft of IP to be $10 billion to $12 billion in the United States, and $50 billion to $60 billion globally.[99] Various industry groups have also honed in on the specific impact of IP theft to themselves. For instance, a 2019 industry report estimated that global digital video piracy reduces revenue to the U.S. content and distribution sectors by between $29 billion and $71 billion per year.[100]

Many stakeholders call for trading partners to have "robust" IPR frameworks to support digital trade. However, they debate the appropriate balance for legal frameworks to protect IPR to incentivize innovation and also set limitations and exceptions to ensure other economically and socially valuable uses. Issues include trading partners' approaches to "fair use"-type exceptions to copyrights and online intermediaries' liability for IPR infringing content and limitations on that liability.[101] Copyright industries assert that that "[t]he success of the creative community in digital trade depends on strong copyright laws and enforcement practices that foster a legitimate online economy."[102] They criticize what they view as overly broad exceptions to copyrights and limitations on the liability of online intermediaries for infringing activity on their networks. In contrast, internet and other technology companies, and some stakeholders support what they view as clear, consistent, and "balanced" copyright protections that include "fair use"[103] and "safe harbors" for ISPs, which they argue are necessary for the smooth functioning of internet services and for developing future technologies.[104]

Other IPR-related barriers to digital trade include government measures, policies, and practices that are intended to promote domestic "indigenous innovation" (i.e., develop, commercialize, and purchase domestic products and technologies) but that can also disadvantage and discriminate against foreign companies. These measures can be linked to "forced" localization barriers to trade. China, for instance, conditions market access, government procurement, and the receipt of certain preferences or benefits on a firm's ability to show that certain IP is developed in China or is owned by or licensed to a Chinese party. Another example is India's data and server localization requirements, which U.S. firms assert hurt market access and innovation in their sector (see above).

National Standards and Burdensome Conformity Assessment

Local or national standards that deviate significantly from recognized international standards may be designed to give a preference to domestic firms and may make it difficult for foreign firms to

IP Commission Report, 2017.

[99] James Lewis, *Economic Impact of Cybercrime–No Slowing Down*, Center for Strategic and International Studies (CSIS) in partnership with McAfee, February 2018.

[100] David Blackburn, Jeffrey A. Eisenach, and David Harrison, *Impact of Digital Video Piracy on the U.S. Economy*, Nera Economic Consulting and Global Innovation Policy Center of U.S. Chamber of Commerce, June 2019.

[101] E.g., through "notice and takedown"-type laws that potentially make online intermediaries liable if they continue to display infringing content after notification from the copyright holder, as well as place limitations on that liability through "safe-harbor" if intermediaries take appropriate action to removing infringing content.

[102] IIPA, "IIPA 2021 Special 301 Report on Copyright Protection and Enforcement," submitted January 28, 2021 to USTR, p. 4.

[103] E.g., exceptions to copyright liability, which allow Internet to scan the Web, make a copy for indexing purposes, and make that copy available for search, without engaging in copyright piracy.

[104] Internet Association, "Submission for the 2021 USTR National Trade Estimate Report," October 29, 2020; Comments of the Computer & Communications Industry Association (CCIA), in response to USTR Request for Public Comments and Notice of a Public Hearing Regarding the 2021 Special 301 Review, Docket No. USTR-2020-0041.

enter a particular market.[105] An ICT product or software that conforms to international standards, for example, may not be able to connect to a local network or device based on a local or proprietary standard. Also, proprietary standards can limit a firm's ability to serve a market if their company practices or assets do not conform with (nor do their personnel have training in) those standards. As a result, U.S. companies may not be able to reach customers or partners in those countries.

Similarly, redundant or burdensome conformity assessment or local registration and testing requirements often add time and expense for a company trying to enter a new market, and serve as a deterrent to foreign companies. For example, India's Compulsory Registration Order (CRO) mandates that manufacturers register their products with laboratories affiliated with or certified by the Bureau of Indian Standards, even if the products have already been certified by accredited international laboratories. The requirement is an often-cited concern for U.S. businesses facing delays getting products to market in India, which may grow as the list of products covered was expanded again in 2020.[106] Qatar requires a license from telecommunications providers to provide Voice over Internet Protocol (VoIP) services, reserving them for companies intending to charter in Qatar, while Egypt requires media outlets, including social media accounts with at least 5,000 subscribers, to pay a fee of 50,000 Egyptian pounds (approximately $2,800) to get a license to gain legal status.[107] If a company is required to provide the source code, proprietary algorithms, or other IP to gain market access, it may fear theft of its IP and not enter that market (see above).

Filtering, Blocking, and Net Neutrality

In some nations, government seeks strict control over digital data within its borders, such as what information people can access online, and how information is shared inside and outside its borders. Government measures that filter or block websites, or otherwise impede access, form another type of nontariff barrier. Such actions often occur in markets where governments maintain tight control over the internet and limit foreign access. For example, China has asserted a desire for "digital sovereignty" and has erected what some experts call the "Great Firewall," a system that limits the ability of Chinese citizens to view certain foreign websites and restricts foreign participation in the internet and many internet tied services. Many Chinese citizens have used virtual private networks (VPNs) and other IP address modification and masking tools to get around the Great Firewall and access websites like Facebook and foreign media sites. VPNs are also frequently used by companies in mainland China to access data outside of China (e.g., information from foreign subsidiaries or partners).[108] Authorities in China have long sought to restrict the use of VPNs to circumvent state internet controls, and a recent change to China's internet filters now more effectively limits the utility of VPNs for accessing foreign websites.[109]

---

[105] Standards refer to product features, technical specifications, or usage guidelines that allow different products or services available to a wide range of users. Standards can be designed to make specific products compatible with others (e.g. electrical outlet and plug configurations) or designed to apply to entire organizations or industrial sectors (e.g. health and safety or IT security standards). For a more in-depth discussion of what constitutes a technical standard, see British Standards Institution, "What is a standard?", accessed March 12, 2021, https://www.bsigroup.com/en-US/Standards/Information-about-standards/What-is-a-standard/.

[106] *2021 National Trade Estimate Report on Foreign Trade Barriers*, Office of the United States Trade Representative, March 2021.

[107] Ibid.

[108] Yu Nakamura, "China's war on VPNs creates havoc at foreign companies," December 17, 2017.

[109] Cate Cadell, "Amid VPN crackdown, China eyes upgrades to Great Firewall," *Reuters*, July 20, 2017; Celia Chen, "Chinese VPN user fined for accessing overseas websites as part of Beijing's ongoing 'clean up' of internet," *South China Morning Post*, January 7, 2019.

One study estimated that China's Great Firewall blocks access to approximately 311,000 separate web domains, including 1,800 of the world's top 100,000 websites, limiting the access of Chinese businesses and consumers to foreign online content, internet infrastructure, and digital services.[110]

While China is the most well-known in its efforts to control its domestic internet, it is not alone in seeking to limit access to websites. For example, Pakistan periodically blocks internet access to services hosting content deemed to be blasphemous or immoral on grounds that such services can be used to undermine national security. Russia's Sovereign Internet Law gives the Russian Government the authority to establish an alternate domain name system for Russia, which would allow them to cut off the Russian segment of the internet from the global internet under certain circumstances.[111] In April 2021, Twitter removed certain "banned content" after Russia's media regulator slowed its internet traffic.[112]

Several U.S. and foreign policymakers have expressed concern about the influence that violent or harmful content online may have upon those who view or read it. In response, some countries have introduced legislation to regulate internet content, for example, to fight the impact and spread of violent material and false information.[113] In the United States, significant First Amendment freedom of speech issues are raised by the prospect of government restrictions on the publication and distribution of speech, even speech that advocates terrorism.[114] As a result, what users can access online may vary across countries, depending on national policy and preferences. These differences illustrate the complexity of the internet and evolving technologies, and the lack of global standards that prevails in other areas of international trade.

National-level net neutrality policies also differ widely. Net neutrality rules govern the management of internet traffic as it passes over broadband internet access services, whether those services are fixed or wireless. Allowing internet access providers to limit or otherwise discriminate against content providers, foreign and domestic, may create a nontariff barrier.[115] In the United States, the Federal Communications Commission (FCC) classification of broadband internet service providers (ISPs) has been controversial domestically and may differ from how U.S. trading partners regulate ISPs.

Cybersecurity Risks

The growth in digital trade has raised issues related to cybersecurity, the act of protecting ICT systems and their contents from cyberattacks. Cyberattacks in general are deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions and disrupting business operations. Cybersecurity can also be an important tool in protecting privacy and preventing unauthorized surveillance or intelligence gathering.[116]

---

[110] Catalin Cimpanu, "China's Great Firewall is blocking around 311,000 domains, 41k by accident," *The Record*, July 11, 2021.

[111] U.S. Trade Representative, *2021 National Trade Estimate Report on Foreign Trade Barriers*, March 2021.

[112] Leonie Cater, "Russia says Twitter complying with most takedown orders," *PoliticoPro*, April, 30, 2021.

[113] European Commission, *European Commission Guidance on Strengthening the Code of Practice on Disinformation*, COM(2021) 262 final, May 26, 2021, and United Kingdom Department for Digital, Culture, Media & Sport. *Draft Online Safety Bill*, CP 405, May 12, 2021.

[114] For more information, see CRS Report R44626, *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes*, by Kathleen Ann Ruane and CRS Report R46751, *Section 230: An Overview*, by Valerie C. Brannon and Eric N. Holmes .

[115] For more information on net neutrality, see CRS Report R40616, *The Federal Net Neutrality Debate: Access to Broadband Networks*, by Patricia Moloney Figliola.

[116] For more information on cybersecurity, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by

Although there is overlap between data protection and privacy, the two are not equivalent. Cybersecurity measures are essential to protect data (e.g., against intrusions or theft by hackers). However, they may not be sufficient to protect privacy.

Cyberattacks can pose broad risks to financial and communication systems, national security, privacy, and digital trade and commerce.[117] According to one study of global organizations, 94% had experienced a business-impacting cyberattack in the prior 12 months.[118] Another survey by IBM Security found that data breach incidents cost companies studied $3.86 million per breach on average, and compromised employee accounts were the most expensive root cause.[119]

Cybersecurity risks run across all industry sectors that rely on digital information. In March 2020, U.S. cybersecurity firm FireEye stated that Chinese state-tied actor APT41 conducted a broad cyber espionage campaign.[120] APT41's targets spanned a diverse set of industries, including finance, construction, health care, manufacturing, and advanced technologies tied to China's industrial planning initiatives, such as *Made in China 2025*.[121] In September 2020, the Department of Justice indicted five Chinese nationals believed to be part of APT41, charging them with multiple counts of conspiracy, aggravated identity theft, money laundering among other charges in connection to cyber intrusion campaigns.[122]

Recent cybersecurity compromises of private sector companies that supply services to the public sector demonstrate the links and potential vulnerability of federal systems and critical infrastructure. For example, SolarWinds makes IT management products for business customers and provides updates and patches to users. When FireEye published research in January 2021 that a malicious actor was exploiting a vulnerability in SolarWinds update service to hack into government and private sector information technology networks, Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive requiring federal agencies to remove certain SolarWinds products from agency networks and take other actions.[123] After a widescale cyber-attack linked to Chinese state-tied cyber threat actors on Microsoft VPN networks across the United States was uncovered in March 2021, the U.S. government and several U.S. allies accused China of "irresponsible and destabilizing behavior in cyberspace."[124] In response, the Department of Justice indicted four PRC nationals who engaged in a state-sponsored hacking

Eric A. Fischer, and CRS In Focus IF10559, *Cybersecurity: A Primer*, by Chris Jaikaran.

[117] Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[118] Tenable Holdings, "Ninety-Four Percent of Organizations Have Experienced At Least One Business-Impacting Cyberattack in the Past 12 Months, According to New Industry Study," August 5, 2020.

[119] IBM, "IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year," July 29, 2020.

[120] Christopher Glyer et al. "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," FireEye, March 25, 2020.

[121] Cybersecurity & Infrastructure Security Agency (CISA), "Alert (AA20-275A) Potential for China Cyber Response to Heightened U.S.–China Tensions," press release, October 20, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-275a.

[122] Office of Public Affairs, Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally, Department of Justice, September 16, 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

[123] For more information, see CRS Insight IN11559, *SolarWinds Attack—No Easy Fix*, by Chris Jaikaran.

[124] The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," *press* release, July 19, 2021, and Zolan Kanno-Youngs and David E. Sanger, "U.S. Accuses China of Hacking Microsoft," *The Washington Post*, August 26, 2021.

campaign affiliated with the PRC Ministry of State Security and the Hainan State Security Department targeting U.S. companies.[125]

Companies that rely on cloud services to store or transmit data may choose to use enhanced encryption to protect the communication and privacy, both internally and of their end customers. This, in turn, may impede law enforcement investigations if they are unable to access the encrypted data.[126] However, restrictions on the ability for a firm to use encryption may make a company vulnerable to cyberattacks or cybertheft, demonstrating the need for policies and regulations to balance competing objectives.

In May 2021, the United States proposed that the WTO Technical Barriers to Trade Committee begin to explore the "landscape of… views on cybersecurity regulation" to identify and promote the application of regulatory approaches that are aligned with WTO principles such as the use of international standards and best practices to maximize security, trade, and innovation outcomes.[127]

U.S. Digital Trade with Key Trading Partners

The European Union (EU) and China are large U.S. digital trade partners and each has presented various challenges for U.S. companies, consumers, and policymakers.

European Union

Differences in U.S. and EU policies have ramifications on digital flows and international trade. The two partners' varying approaches to digital trade, privacy, and national security, have, at times, threatened to disrupt U.S.-EU data flows.

The United States and the EU have a significant, highly integrated economic relationship and are each other's largest overall trade and foreign direct investment (FDI) partners.[128] In 2020, U.S. goods and services exports to the EU were more than double U.S. exports to China and imports from the EU were 17% greater than those from China.[129] Cross-border data flows between the United States and EU are among the highest in the world. U.S.-EU trade of ICT services and potentially ICT-enabled services was over $264 billion in 2020.[130] The United States maintains a large digital trade surplus over the EU (see **Figure 4**). Two of the top five e-commerce retailers in Europe were U.S. firms in 2020.[131]

[125] Office of Public Affairs, Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research, Department of Justice, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

[126] For more information on encryption, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea, and CRS Report R44407, *Encryption: Selected Legal Issues*, by Richard M. Thompson II and Chris Jaikaran.

[127] United States, *Proposal on Regulatory Cooperation Cybersecurity of Software-Enabled and/or Network Connected Goods*, WTO G/TBT/W/747, May 17, 2021.

[128] CRS In Focus IF10930, *U.S.-EU Trade and Investment Ties: Magnitude and Scope*, by Shayerah I. Akhtar.

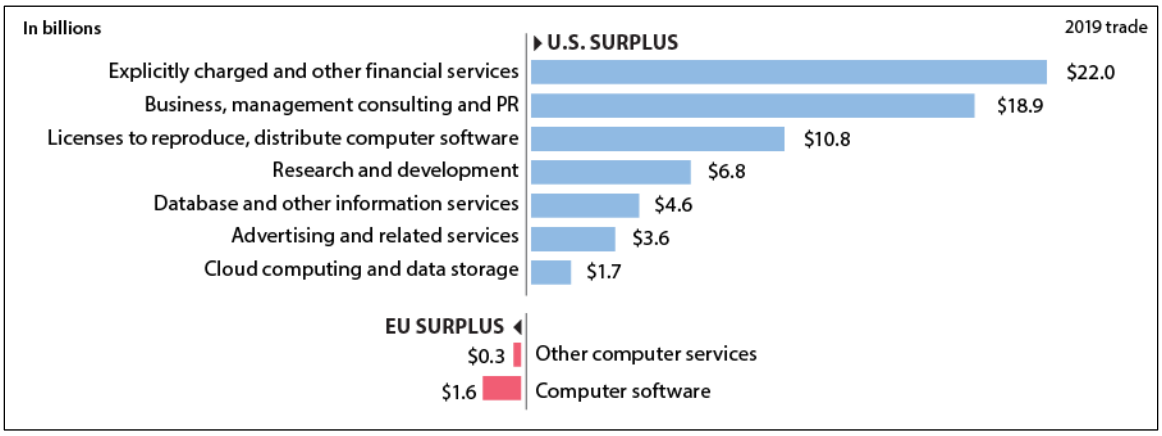
[129] U.S. Bureau of Economic Analysis, Table 1.5. U.S. International Trade in Goods and Services by Area and Country, December 21, 2021.

[130] U.S. Bureau of Economic Analysis, Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Country or Affiliation, July 2, 2021. Data includes the UK.

[131] Retail-Index, Top 100 E-Commerce Retailers in Europe, https://www.retail-index.com/E-commerceretail.aspx.

Figure 4. Trans-Atlantic Digitally Enabled Services Trade Flows

2019



Source: Mark Scott, "Digital Bridge," *Politico*, April 1, 2021, based on U.S. Bureau of Economic Analysis data.

General Data Protection Regulation (GDPR)

Differences in U.S. and EU approaches to data privacy and protection have long been sticking points in U.S.-EU relations. The EU's General Data Protection Regulation (GDPR), effective May 2018, established rules for EU member states to safeguard individuals' personal data.[132] The GDPR is a comprehensive privacy regime that builds on previous EU data protection rules. It grants new rights to individuals to control personal data and creates specific new data protection requirements.

The GDPR applies to: (1) all businesses and organizations with an EU establishment that process (perform operations on) personal data of individuals (or "data subjects") in the EU, regardless of where the actual processing of the data takes place; and (2) entities outside the EU that offer goods or services (for payment or for free) to individuals in the EU or monitor the behavior of individuals in the EU. U.S. businesses have raised concerns about the GDPR's extraterritorial implications. Multiple member states have conducted investigations into U.S. firms for possible breaches of GDPR. In May 2021, the European Data Protection Supervisor opened investigations into Amazon Web Services and Microsoft.[133]

Some experts contend that the GDPR may effectively set new global data privacy standards, since many companies and organizations strive for GDPR compliance to avoid being shut out of the EU market, fined, or otherwise penalized. In addition, some countries outside of the EU have imitated all or parts of the GDPR in their own privacy regulatory and legislative efforts. For example, California's privacy legislation is based in part on the EU's GDPR, and Virginia enacted similar, though less comprehensive, privacy legislation.[134]

[132] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[133] European Data Protection Supervisor, "The EDPS opens two investigations following the "Schrems II" Judgement," press release, May 27, 2021.

[134] California Privacy Rights Act is codified as Cal. Civ. Code §§ 1798.100-1798.199.100 and Virginia Consumer Data Protection Act, 2021 ch. 35 (to be codified at Va. Code Ann. §§ 59.1-571-59.1-581).

EU-U.S. Privacy Shield

To bridge differences between U.S. and EU approaches to data privacy and protection, and to enable data transfers, the United States and the EU have concluded data-sharing accords in both the commercial and law enforcement sectors. In July 2020, the Court of Justice of the European Union (CJEU) invalidated the most recent U.S.-EU commercial data transfer accord, the Privacy Shield Framework, which had been in force since 2016. The Privacy Shield had provided over 5,000 mostly small and mid-sized entities a mechanism to transfer EU citizens' personal data to the United States while complying with EU data protection rules. The CJEU found that Privacy Shield failed to meet EU GDPR data protection standards, given the breadth of U.S. data collection powers authorized in U.S. electronic surveillance laws and the lack of redress options for EU citizens. The CJEU ruling creates legal uncertainty for many firms engaged in transatlantic trade. Although U.S. and EU officials are negotiating on how to update or replace Privacy Shield, the CJEU decision demonstrates the potential difficulties that the parties face in attempting to overcome differences in their internet regimes and approaches to technology regulation given the lack of international data privacy rules or standards.

For more information on U.S.-EU data flows, see CRS In Focus IF11613, *U.S.-EU Privacy Shield*, by Rachel F. Fefer and Kristin Archick.

The EU's Digital Policy

The EU's executive branch, the European Commission, issued its 2020 digital policy roadmap, "Shaping Europe's Digital Future," to strengthen the EU economy and improve the region's digital competitiveness, especially with the United States and China.[135] EU policymakers have talked about "open strategic autonomy," a term that reflects the desire for the EU to be able to act independently on the world stage, exerting leadership in line with EU interests and values in a wide range of areas, including in the trade, digital, and industrial policy spheres. Similar to the GDPR and data protection rules, the EU hopes to set global precedents for international digital rules in the areas of online competition and content, among others.

The roadmap sets out various initiatives that aim to forge a "fair and competitive" EU digital economy. The initiatives build on previous work, such as the GDPR, to further the EU's single market and seek to drive innovation, address online platforms, develop digital services, promote competition, and protect data. Some of the efforts that are of particular congressional interest are described below.

- The draft "Digital Markets Act (DMA)" aims to establish competition rules for large online platforms.[136] The DMA includes new ex ante rules[137] for platforms with a list of "do's and don'ts" for designated online "gatekeepers," identifying specific services that are allowed or prohibited. Gatekeepers would be designated by the European Commission according to quantitative and qualitative criteria.

[135] European Commission, "Shaping Europe's digital future," February 2020, at https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf, and https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en. For more information, see https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy.

[136] The Digital Markets Act (DMA), published December 15, 2020, by the European Commission, would establish competition rules for certain online platforms. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)*, COM/2020/842 final, December 15, 2020, at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN. For more information, see European Commission, "The Digital Markets Act: ensuring fair and open digital markets," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

[137] Regulation is commonly referred to as an ex-ante ("existing before the event") government tool; competition rules and enforcement are commonly referred to as an ex-post ("after the fact").

Violations of the rules could result in fines of up to 10% of a company's total worldwide annual revenue. In some cases, the commission could impose behavioral or structural penalties (e.g., divestiture of certain businesses).

- The draft "Digital Services Act (DSA)" seeks to set liability rules related to illegal online content and products, transparency obligations, and other requirements for all online intermediary services.[138] The DSA includes rules for all online intermediary services doing business in the EU, but the requirements vary by company size and role in the digital marketplace, with four distinct tiers identified in the draft.
- The proposed ePrivacy Regulation would ensure the privacy of electronic communications by requiring traditional telecommunications providers, as well as messaging services (e.g., WhatsApp and SnapChat), to obtain explicit user consent for online tracking (use of cookies), and limit the amount of time that the tracking data may be stored.[139]
- The draft "Data Governance Act" aims to set the legal foundation for a single market for data sharing across the EU, with a focus on public and industrial, nonpersonal data, while also encouraging "data altruism" by EU individuals to share their personal data for "the common good"; all data sharing by companies and individuals would be voluntary. [140]
- The proposal on AI seeks to ensure "trustworthy AI" and a human-centric approach.[141] The draft framework uses a risk-based approach to establish four tiers of risk depending on the function of the AI system, with requirements varying by tier.

Each proposed or draft regulation would take time to progress to enactment into EU law, potentially months or years, because it would require the approval of each member state and the European Parliament.[142] Whether each regulation once finalized and enacted will supersede

[138] The Digital Services Act (DSA), published December 15, 2020, by the European Commission, would set rules for online intermediaries. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM/2020/842 final, December 15, 2020, at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN. For more information, see European Commission, "The Digital Services Act: ensuring a safe and accountable online environment," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

[139] For more information on the ePrivacy Regulation see, https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

[140] The proposed Data Governance Act, published November 25, 2020, by the European Commission, would set rules for data-sharing within the EU. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)*, COM/2020/767 final, November 25, 2020, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

[141] The proposed Artificial Intelligence Act, published April 21, 2021, by the European Commission would set the legal framework for AI. European Commission, *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, April 21, 2021, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

[142] For more information on the EU legislative process, see https://ec.europa.eu/info/law/law-making-process/adopting-eu-law_en#:~:text=Most%20EU%20laws%20are%20adopted%20using%20the%20ordinary,in%20order%20for%20it%20to%20become%20EU%20law. Also see CRS In Focus IF11211, *The European Parliament and U.S. Interests*, by Kristin Archick.

national member state laws, and the amount of flexibility member states will have, remain to be seen.[143]

New EU Copyright Rules

On April 15, 2019, the EU adopted new rules to modernize its copyright laws to adapt to the digital environment, including creating a fairer marketplace for online content for creators and press.[144] The directive introduces an EU-wide "neighboring right" to allow news publishers to be compensated for the use of their articles by online platforms, as well provide for journalists to receive an appropriate share of the revenues generated. News platforms such as Google and Facebook have to negotiate licenses from newspapers and other publishers for showing content that is less than two-years-old on their news feeds. Short extracts from press publications—sometimes called "snippets"—are outside of the scope of the rule. The directive also reinforces the position of creators and right holders to negotiate and secure compensation for online use of their content hosted in the EU by major content platforms such as YouTube. Under the much-debated Article 17, if no licensing agreement exists between creators and the online sharing platforms (e.g., YouTube), these platforms must demonstrate "best efforts" to remove copyright materials if they are notified of infringing uploads. Newer and smaller platforms are not subject to all of these requirements. The directive addresses other digital copyright issues as well.

Debate over the rules is ongoing in the EU and among other stakeholders, including U.S. companies. Supporters believe that the rules will help facilitate the licensing and distribution of digital content and support innovation. Critics voice concern that the rules will block content and create compliance burdens. Much of the recent debate has focused on Article 17, despite the European Commission's efforts to clarify that the obligations apply to online service providers that profit from user-uploaded copyright work on their platform—and not, for instance, to not-for-profit online encyclopedias or educational repositories, open source software developing platforms, and e-commerce marketplaces and certain other exceptions, as well as to certain "legitimate uses" of content, such as for quotation or criticism.[145]

The United States is continuing to monitor developments related to the copyright rules and to engage with the EU to address U.S. stakeholders' equities.[146] France has been a recent "testing ground" for how implementation of the copyright rules may affect certain U.S. commercial interests.[147] In July 2021, France fined Google $593 million for allegedly violating orders to negotiate "in good faith" paid deals with news publishers for the right to show snippets of their content in its search results. Google voiced disapproval of the decision, but recently concluded a five-year licensing deal with Agence France-Press.[148] In June 2021, the CJEU ruled that platforms such as YouTube cannot be held liable for user uploading unauthorized works, although they are responsible for taking action to remove or block content. The CJEU ruling does not take into

[143] For more information on the EU digital policies, see CRS Report R46732, *EU Digital Policy and International Trade*, by Rachel F. Fefer.

[144] European Commission, "New EU Copyright Rules That Will Benefit Creators, Businesses and Consumers Start to Apply," press release, June 4, 2021.

[145] Foo Yun Chee, "Critics Still Unhappy as EU Clarifies Revamped Copyright Rules," June 4, 2021, Reuters.

[146] USTR, 2021 National Trade Estimate Report on Foreign Trade Barriers, March 2021.

[147] Laura Kayli, "Europe's Controversial Copyright Reform Turns 1 Amid Ongoing Tensions," POLITICO, April 15, 2020.

[148] Sam Schechner, "Google Fined $593 Million in France Over Treatment of News Publishers," July 13, 2021, The Wall Street Journal.

account the new copyright directive.[149] In other developments, following Spain's adoption of the new EU copyright law, Google News plans to return to Spain after closing its services in 2014; Spain had passed a law requiring news aggregators to pay a central license fee to Spanish news organizations for using their stories, while the new law adopted by Spain allows news aggregators to negotiate licensing fees directly with news organizations.[150]

U.S.-EU Digital Cooperation

Despite close economic ties, differences between the United States and EU in their approaches to data flows and digital trade have caused friction in U.S.-EU economic and security relations. The Biden Administration has engaged with the EU to create digital specific bilateral forums.

At the U.S.-EU Summit in June 2021, the parties agreed to intensify cooperation in multiple areas and formed new forums to focus on specific issues including digital.

- U.S.-EU Trade and Technology Council (TTC) to address multiple trade and technology issues to promote "a democratic model of digital governance." The TTC aims to "strengthen global cooperation on technology, digital issues, and supply chains;" "support collaborative research and exchanges;" and "cooperate on compatible and international standards development" among other issues.
- U.S.-EU Joint Technology Competition Policy Dialogue to focus on approaches to competition policy and enforcement.

The parties also agreed to "work together to strengthen legal certainty in Transatlantic flows of personal data" without specifically referencing the U.S.-EU Privacy Shield.[151] The new dialogues and political agreement may add momentum to build greater alignment and understanding on digital policy between the United States and the EU, and create opportunities bring in other allies and partners.

Digital trade issues also have featured in past U.S.-EU trade agreement negotiation efforts. The Biden Administration has not indicated whether it wants continue the U.S. trade agreement negotiations with the EU that the Trump Administration notified to Congress under TPA, which contemplated a wide-ranging trade agreement addressing digital trade and other issues.[152] Previously, under the Obama Administration, the United States and the EU sought to negotiate the Transatlantic Trade and Investment Partnership (T-TIP) which would have included treatment of digital trade issues, including market access for digital products, IPR protection and enforcement, cybersecurity, and regulatory cooperation, among other things.[153] Among other issues, discussions

[149] Ryan Browne, "YouTube Secures a Big Win in the EU Over Copyright," CNBC, June 22, 2021.

[150] Tom Bateman, "Google News Returns to Spain After the Country Adopts New EU Copyright Law," *EuroNews*, November 4, 2021.

[151] The White House, *U.S.-EU Summit Statement, Towards a Renewed Transatlantic Partnership*, Press release, Washington, DC, June 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

[152] USTR, "United States-European Union Negotiations: Summary of Specific Negotiating Objectives," January 2019.

[153] Under the Obama Administration, a U.S. goal for T-TIP had been to develop "appropriate provisions to facilitate the use of electronic commerce to support goods and services trade, including through commitments not to impose customs duties on digital products or unjustifiably discriminate among products delivered electronically." USTR, "U.S. Objectives, U.S. Benefits in the Transatlantic Trade and Investment Partnership: A Detailed View," fact sheet, March 2014.

on digital trade faced complications due to EU engagement on parallel issues in its internal market and EU concerns over U.S. government surveillance.

China

China presents a number of significant opportunities and challenges for the United States in digital trade. The digitization of certain parts of the Chinese economy, coupled with a large and increasingly prosperous population, has led to a surge in the number of Chinese internet users and made China a major source of global ecommerce. Since 2000, China's total number of internet users has grown from 21.5 million to an estimated 1 billion, according to official statistics published by a central government department under the Cyberspace Administration of China (CAC). This rapid growth in internet users is primarily seen by analysts as a result of a concerted government focus on expanding mobile internet access across the country, particularly in rural and remote areas.[154] Chinese data on mobile app use also highlights the growth of several discrete service and product areas across China's economy. Approximately 99.7% of China's internet users access the internet via smartphone. As of February 2021, online games constituted approximately 25% of all mobile phone apps on Chinese mobile app stores, while e-commerce and consumer services apps represented 9.9% and 9% of mobile apps in China, respectively, according to Chinese government data.[155]

China's e-commerce market is currently the world's largest in terms of both transactions and potential consumers, surpassing those of the United States, UK, Japan, Germany, and France combined.[156] China is home to approximately 710 million e-commerce customers, according to data compiled by the U.S. Department of Commerce, and China's online retail transactions reached $1.93 trillion in 2019 (approximately $33 billion of which were cross-border transactions) and are projected to reach $4.09 trillion by 2023.[157] Many market analysts contend that the size of China's e-commerce consumer base, combined with the rapid "digitization" of daily goods and services transactions, will continue to drive long-term innovation in China's digital economy.[158]

U.S. firms may benefit from the expanding digital trade in China, but they also face numerous challenges in the Chinese market, most notably several NTBs that limit the ability of foreign firms to compete in China's digital services markets. In its 2021 annual report on trade barriers, USTR identified several significant NTBs that hamper U.S. firms operating in China's digital markets, including China's emerging cybersecurity and data governance regime (discussed below), investment restrictions in China's technology and ICT sectors, and new encryption requirements that mandate the use of indigenous encryption algorithms, among others.[159] More

[154] CSIS China Power Team, "How Web-Connected is China?" *Center for Strategic and International Studies*, updated May 25, 2021, https://chinapower.csis.org/web-connectedness/.

[155] China Internet Network Information Center, *The 47th Statistical Report on China's Internet Development,* February 2021, available at https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172744.pdf.

[156] International Trade Administration, "China-Country Commercial Guide, eCommerce," last updated February 3, 2021, https://www.trade.gov/country-commercial-guides/china-ecommerce.

[157] Ibid.

[158] McKinsey & Company, "The Future of Digital Innovation in China: Megatrends Shaping One of the World's Fastest Evolving Digital Ecosystems," September 30, 2021, https://www.mckinsey.com/featured-insights/china/the-future-of-digital-innovation-in-china-megatrends-shaping-one-of-the-worlds-fastest-evolving-digital-ecosystems?cid=other-eml-alt-mip-mck&hdpid=50658e70-0465-4138-aa00-0c4e815cdba8&hctky=2915206&hlkid=26e2f1d89ccf4903b94cf9217466c47d.

[159] Office of the United States Trade Representative, *2021 National Trade Estimate Report on Foreign Trade Barriers,*

broadly, China also maintains investment restrictions on foreign investment in most internet and telecommunications sectors, and the limited extent to which foreign firms are allowed to participate in these industries is often conditioned on various localization and joint venture requirements.[160] USTR's findings also note that China has generally failed to notify new technical regulations governing cybersecurity and data protection to the WTO Committee on Technical Barriers to Trade, a process that China had previously agreed to follow.

According to an annual survey of U.S. firms operating in China conducted by the American Chamber of Commerce in China (AmCham China), approximately one-third of U.S. firms operating in technology and other research-intensive industries named data security and increasing protectionism as among their top business challenges in China. Additionally, a quarter of U.S. firms operating in China's services sector pointed to internet access quality, censorship, and data security as among the top challenges facing their operations in China.[161] In general, one in five respondents to the AmCham China survey noted that data localization requirements have had an "extremely negative" impact on their competitiveness and operations in China. Other concerns identified by firms surveyed include concerns regarding new data privacy regulations, hardware and software procurement restrictions on information systems, and IP leakage and data security concerns during third party reviews of products and software **(Table I)**:

Table 1. American Chamber of Commerce in China 2021 Business Survey

Percentage of Respondents Indicating Concerns Related to China's Data Governance Regime

To what degree do the following Cybersecurity Law-related issues negatively affect your company's competitiveness and operations in China?	Not at all	Significantly	Extremely
Data localization requirements	34%	44%	21%
Cybersecurity rules on protection of critical information infrastructure and important data	35%	48%	16%
Data security/IP leakage as a result of third party reviews	40%	46%	14%
Hardware/software procurement restrictions and other "secure and controllable" policies	46%	43%	12%
Compliance concerns due to vague implementing regulations	31%	54%	16%
Data privacy regulations	30%	54%	16%

Source: American Chamber of Commerce in China 2021 Business Climate Survey.

Foreign firms operating in China have often chosen to operate in Hong Kong or invest in additional offices there in order to mitigate the effects of China's internet restrictions and data localization requirements, which have limited the connectivity of internet users with IP addresses based in mainland China. Several U.S. social media and internet companies whose services are restricted in mainland China—including Facebook, Twitter, Google, and Amazon Web Services, among others—maintain offices in Hong Kong in order to offer services within the city and conduct less restricted ancillary business, such as advertising, in mainland China.

March 2021 (Washington, DC), https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf, pp. 94-130.

[160] For more details on these investment restrictions, see CRS Report R46915, *China's Recent Trade Measures and Countermeasures: Issues for Congress*, by Karen M. Sutter, pp. 16-19.

[161] American Chamber of Commerce in China, "2021 China Business Climate Survey Report," March 2021, https://www.amchamchina.org/climate-survey/2021-business-climate-survey/.

Following the Chinese government's crackdown on pro-democracy protests in Hong Kong in 2019 and 2020, however, several experts and members of the international business community in Hong Kong have expressed concerns about the erosion of certain business freedoms long enjoyed by multinational firms operating in Hong Kong, including a lack of cross-border data and internet content controls.[162] The Chinese government's imposition of a new National Security Law in Hong Kong has intensified these concerns.[163] Several of U.S. technology firms, most notably Facebook and Twitter, have announced that they are considering exiting Hong Kong in response to certain moves by Hong Kong regulators to introduce new restrictions on internet activities that could incite "illegal acts" as defined by the new National Security Law, which include many forms of social organizing often conducted using social media services.[164] In January 2021, Hong Kong Broadband Network (HKBN), the territory's primary internet service provider, announced that it would block access to or remove domains that could incite "illegal acts," which further fueled concerns about an expansion of Beijing's internet censorship policies into Hong Kong.[165]

"Cyber Sovereignty" and China's Involvement in Global Internet Governance

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 "Cyber Sovereignty.[166] Although various definitions of the term have been offered by China's State Council and its subordinate ministries, the most expansive definition of the principle of cyber sovereignty is currently outlined in the Chinese government's 2017 *International Strategy of Cooperation on Cyberspace*. The document outlines a vision of cyber sovereignty that emphasizes the rights of individual governments to control their ICT infrastructure:

> *National governments are entitled to administer cyberspace in accordance with law. They exercise jurisdiction over ICT infrastructure, resources and activities within their territories, and are entitled to protect their ICT systems and resources from threat, disruption, attack and destruction so as to safeguard citizens' legitimate rights and interests in cyberspace. National governments are entitled to enact public policies, laws, and regulations with no foreign interference. Countries should exercise their rights based on the principle of sovereign equality and also perform their due duties. No country should*

[162] American Chamber of Commerce in Hong Kong, "Should I Stay or Should I Go? A Temperature Testing Survey of Expats in Hong Kong," May 2021, https://www.amcham.org.hk/sites/default/files/content-files/Survey/202105%20AmCham%20Survey%20-%20Should%20I%20Stay%20or%20Should%20I%20Go%20-%20FINAL_1.pdf; Newley Purnell, "Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws," *The Wall Street Journal*, July 5, 2021, https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036.

[163] Kari Soo Lindberg, Natalie Lung and Pablo Robles, "How Hong Kong's National Security Law is Changing Everything," *Bloomberg*, October 5, 2021, https://www.bloomberg.com/graphics/2021-hong-kong-national-security-law-arrests/.

[164] Reuters, "Asia industry group warns privacy law changes may force tech firms to quit Hong Kong," July 5, 2021, https://www.reuters.com/world/china/facebook-google-twitter-say-could-quit-hong-kong-over-proposed-data-laws-wsj-2021-07-05/.

[165] Jessie Pang, "Hong Kong censorship debate grows as internet firm says can block 'illegal acts'," *Reuters*, January 15, 2021, https://www.reuters.com/article/us-hong-kong-security-censorship/hong-kong-censorship-debate-grows-as-internet-firm-says-can-block-illegal-acts-idUSKBN29K0ZM.

[166] The principle has also been translated in some publications as "Internet Sovereignty (网络主权 *wangluo zhuquan*)." This report uses "Cyber Sovereignty," which matches the term for the principle used in the Chinese version of the 2017 International Strategy for Cooperation on Cyberspace (网络空间的主权 *wangluo kongjian zhuquan*).

> *use ICT to interfere in other countries' internal affairs or leverage its advantage to undermine the security of other countries' ICT product and service supply chain.*[167]

The document also asserts that "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."[168] Some analysts contend that the Chinese government's definition of cyber sovereignty represents an assertion that governments should have control over the internet and data flows generated by users within their borders.[169] Chinese delegations to international organizations that set global internet standards, such as the International Telecommunications Union (ITU) and Internet Corporation for Assigned Names and Numbers (ICANN), have advanced proposals that align with the Chinese government's view of internet sovereignty.[170] Cyber sovereignty is also a key element in China's commercial expansion into sectors of the global digital economy, such as cloud computing. Huawei, a major Chinese provider of ICT infrastructure and cloud services globally, supplies artificial intelligence and surveillance technology and services to governments in packages that are often designed to be centrally controlled by government security services.[171]

In addition to its potential international implications, some see China's invocation of "sovereignty" in its new data security and cybersecurity laws as an attempt by the government to control information that is deemed a threat to social stability.[172] Some critics of China's push for global standards that conform to its principles of cyber sovereignty have characterized the effort as promoting "digital authoritarianism."[173] Other critics of China's cyber sovereignty principle view it as an attempt by the government to limit market access by foreign internet, digital, and high technology firms in China and to boost Chinese firms, reduce China's dependence on foreign technology, and exercise more comprehensive control over market entry in expanding IT and digital services sectors.[174]

China's Emerging Cyberspace and Data Protection Regime

China's leaders have emphasized the importance of data over the past several years, and have made efforts to shape China's emerging digital economy through a series of new laws and

---

[167] Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace," January 3, 2017, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

[168] Ibid.

[169] Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," *National Bureau of Asian Research*, August 25, 2020, https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/.

[170] Rogier Creemers, "China's Approach to Cyber Sovereignty," *Konrad-Adenauer-Stiftung*, November 25, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

[171] Adam Segal, *China's Alternative Cyber Governance Regime*, testimony before the U.S.-China Economic and Security Review Commission, March 13, 2020, https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

[172] Elliott Zaagman, "Cyber sovereignty cuts both ways," *The Interpreter (Lowy Institute)*, August 7, 2020, https://www.lowyinstitute.org/the-interpreter/cyber-sovereignty-cuts-both-ways.

[173] U.S. Congress, Senate Committee on Foreign Relations, *The New Big Brother: China and Digital Authoritarianism*, 116th Congress, 2nd sess., July 21, 2020.

[174] Rush Doshi, Emily De La Bruyere, Nathan Picarsic, and John Ferguson, "China As A "Cyber Great Power": Beijing's Two Voices In Telecommunications," *Brookings Institution*, April 5, 2021, https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.

implementing regulations that define how businesses can generate, process, and sell data and information. In addition to various industry and government-mandated cybersecurity standards, China's leaders have pushed to define the scope of China's digital economy by enacting new laws governing various aspects of China's internet infrastructure.

Following the enactment of an updated National Security Law in 2015 and new Cybersecurity Law in 2018, China's National People's Congress in 2021 passed a new Data Security Law and Personal Information Protection Law. The Data Security Law and Personal Information Protection Law are both in effect as of November 1, 2021. These new laws governing cyberspace and the generation and use of data contain several provisions that could create additional regulatory barriers to digital trade with China and limit the ability of U.S. firms to provide hardware, software, and services in China. Many of these laws are premised on a now-ubiquitous principle across Chinese tech regulations that critical information infrastructure should be "secure and controllable," a term that has not been precisely defined by Chinese authorities but which has been developed and applied in the market since at least 2007, including in China's updated 2015 National Security Law.[175] Other proposals of concern to U.S. firms appear to lay out policies that would require foreign firms across a range of technology sectors to share proprietary information as part of new licensing practices (See **text box**). Laws that have been enacted or passed in China that present challenges to accessing China's digital markets include

- **Data Security Law of the People's Republic of China** regulates all "data activities" conducted within China's borders, and notably covers data activities conducted outside of China that may "... harm the national security of the People's Republic of China, or the legitimate rights of Chinese citizens or entities."[176] The law is the first to regulate "data transactions" in China, and requires China's State Council to establish data transaction management systems and "... cultivate a data transaction market."[177]

Some analysts contend that the new law could create an environment conducive to further expansion of digital trade and e-commerce in China by providing clear regulations and standards for businesses handling Chinese user data. Others argue that the law's emphasis on state control and review of data, coupled with its explicit extraterritoriality, could make it more difficult for multinational firms handling Chinese user data in any capacity to conduct operations in China.[178] For example, following LinkedIn's decision to end its China operations in October 2021, the firm

[175] For more on China's localization requirements, see CRS Report R46915, *China's Recent Trade Measures and Countermeasures: Issues for Congress*, by Karen M. Sutter, pp. 22-28.

[176] Passed by the National People's Congress (or NPC, China's primary legislative body) in June 2021 and effective September 2021. The law's definition of "data activities" includes data usage, storage, collection, processing provision, disclosure, or transmission. For a summary of key provisions in the Data Security Law, see Hui Xu and Kieran Donovan, "China's New Data Security Law: What to Know," *Latham & Watkins*, July 21, 2021, https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to-know.

[177] Article 19 of the Data Security Law of the People's Republic of China, for translation of the full law see "Data Security Law of the People's Republic of China (Translation)," *Stanford DigiChina*, June 29, 2021, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

[178] Camille Boullenois, "China's Data Strategy: Creating a state-led market," *EU Institute for Security Studies*, October 6, 2021, https://www.iss.europa.eu/content/chinas-data-strategy#_unleashing_the_potential_of_data_resources; Katja Drinhausen and John Lee, "The CCP in 2021: smart governance, cyber sovereignty and tech supremacy," *Mercator Institute for China Studies*, June 15, 2021, https://merics.org/en/ccp-2021-smart-governance-cyber-sovereignty-and-tech-supremacy.

cited concerns about China's new data localization and security requirements as a significant factor in its decision.[179]

- **Personal Information Protection Law of the People's Republic of China (PIPL)** imposes new obligations on actors that handle the personal data of Chinese individuals. Similar to China's Data Security Law, the PIPL has a dimension of extraterritoriality and applies to the handling and processing of personal information generated by Chinese individuals both inside and outside of China.[180] In addition to further rules and restrictions on cross-border data transfers of personal data, the PIPL also includes several provisions governing the use of "automated decision-making" using the personal information of Chinese individuals, which many analysts contend could have a significant impact on the use of algorithms for advertising or market research purposes.[181]

Several experts note that the introduction of the PIPL follows several years of widespread concern among both Chinese consumers and regulators that companies that handle personal information and user data in China have not been taking adequate steps to protect it. Instead, some analysts contend that provisions in the PIPL might be an effort by the Chinese government to leverage broad concerns about data privacy to exert pressure on the private sector and create more visibility for regulators into the data generated and processed by popular apps and internet services. For example, several of China's largest tech and e-commerce firms, such as Tencent, Alibaba, and Baidu, had historically been reticent to share details about their handling of consumer data with regulators, but have since agreed to comply with regulators following the release of the draft PIPL giving the state wider access to personal data.[182]

Chinese consumers are also becoming more concerned about the handling of their personal information as commercial surveillance technology has become more common in China: in 2020, a Chinese visitor to a zoo in Hangzhou won a lawsuit against the zoo following a provincial court's decision that the zoo's use of facial recognition technology "... exceeded the legally necessary requirements."[183] Several observers note that the PIPL, which further codifies a principle of minimum necessity governing the collection of personal information, shares several points of similarity with GDPR.[184] However, unlike GDPR which is focused on consumer rights,

[179] Karen Weise and Paul Mozur, "LinkedIn to Shut Down Service in China, Citing 'Challenging' Environment," *NEw York Times*, October 14, 2021, https://www.nytimes.com/2021/10/14/technology/linkedin-china-microsoft.html.

[180] Passed by the NPC in August 2021 and effective November 2021. For a full translation of the law, see Rogier Creemers and Graham Webster, "Translation: Personal Information Protection Law of the People's Republic of China—Effective Nov. 1, 2021," *Stanford DigiChina*, August 20, 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[181] Alexa Lee et. al, "Seven Major Changes in China's Finalized Personal Information Protection Law," *Stanford DigiChina*, September 15, 2021, https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/.

[182] For example, Chinese authorities have been exerting pressure for several years on Ant Group, Tencent, and e-commerce giant JD.com to share consumer credit data with regulators. For more, see Julie Zhu, "China to push its tech giants to share consumer credit data—sources," *Reuters*, January 11, 2021, https://www.reuters.com/world/china/exclusive-china-push-its-tech-giants-share-consumer-credit-data-sources-2021-01-11/.

[183] Tracy Qu, "Chinese court orders wildlife park to delete facial recognition data as privacy concerns grow among Chinese citizens," *South China Morning Post*, November 23, 2020, https://www.scmp.com/tech/big-tech/article/3110981/chinese-court-orders-wildlife-park-delete-facial-recognition-data.

[184] Masha Borak, "China's privacy law borrows a page from Europe's GDPR but it goes further as Beijing shores up data security," *South China Morning Post*, August 26, 2021, https://www.scmp.com/tech/tech-war/article/3146523/chinas-privacy-law-borrows-page-europes-gdpr-it-goes-further-beijing; Gibson Dunn, China Passes the Personal Information Protection Law, to Take Effect on November 1," September 10, 2021, https://www.gibsondunn.com/china-

the PIPL does not appear to contain significant or meaningful constraints on the Chinese government's ability to collect and analyze data—while the law does contain provisions that create a framework for intra-governmental standards for government agencies managing data generated by users in China, these appear to be primarily focused on outlining the roles of particular ministries and departments in handling and processing data.[185]

- **Cybersecurity Law of the People's Republic of China** ascertains the principles of cyberspace sovereignty;[186] defines the security-related obligations of network product and service providers; further enhances the rules for protection of personal information; establishes a framework of security protection for "critical information infrastructure"; and establishes regulations pertaining to cross-border transmissions of important data by critical information infrastructure.[187] Following the law's entry into effect, several experts and business advocacy groups argued that its lack of a clear definition for what constitutes "critical information infrastructure" could lead to additional compliance risks for firms that handle or generate data in China (see **text box**).[188] For example, CAC or the PRC government subjected Chinese ride-hailing firm *Didi Chuxing* to a cybersecurity review following concerns expressed by CAC and other regulatory agencies about its handling of Chinese user data in the wake of an initial public offering (IPO) on the New York Stock Exchange, resulting in a significant drop in Didi's stock price immediately following its IPO and its temporary removal from app stores in China. [189]
- **National Security Law of the People's Republic of China** emphasizes the state's role in driving innovation and reviewing "foreign commercial investment, special items and technologies, internet information technology products and services, projects involving national security matters, as well as other major matters and activities, that impact or might impact national security."[190] The law has served as a cornerstone of the Chinese government's emerging data governance regime—one article establishes the goal of "elevating the capability to protect network and information security," as well as "achieving the ***security***

passes-the-personal-information-protection-law-to-take-effect-on-november-1/.

[185] Rogier Creemers, "China's Emerging Data Protection Framework," November 16, 2021, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684.

[186] Passed by the NPC on November 7, 2016, and effective June 1, 2017. Article 1 states: "This law is formulated so as to ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization."

[187] Deloitte, "A new era for Cybersecurity in China," November 2017, available at https://www2.deloitte.com/cn/en/pages/risk/articles/new-era-cybersecurity-law.html.

[188] Daniel Rechtschaffen, "Why China's Data Regulations are a Compliance Nightmare for Companies," *The Diplomat*, June 27, 2019, https://thediplomat.com/2019/06/why-chinas-data-regulations-are-a-compliance-nightmare-for-companies/.

[189] Yuan Yang, "Didi shares tumble as Chinese regulators launch data investigation," *Financial Times*, July 2, 2021, https://www.ft.com/content/0d1d96e7-6b56-4c92-b6f1-b0f93d8b5e72; Sophie You and Emilia Jin, "China Removes Didi from App Stores: What We Learned from the Case and China's Cybersecurity Regime," *China Briefing*, August 13, 2021, https://www.china-briefing.com/news/china-removes-didi-from-app-stores-lessons-learned-chinas-cybersecurity-regime/.

[190] Initially enacted in 1993 and most recently revised in 2015. Article 59, translation from the Council on Foreign Relations, *National Security Law of the People's Republic of China*, July 1, 2015, http://www.cfr.org/homeland-security/national-security-law-peoples-republic-china/p36775.

and controllability of core network and information techniques, key infrastructure, information systems in important fields and data," among other measures.[191]

China's Cybersecurity Law, Joint Ventures, and Localization in China: The Case of Apple's Guiyang Data Center

Over the decade following the iPhone's launch in China in 2009, China quickly shifted from primarily a supplier of intermediate inputs for iPhones and other Apple products to a significant consumer of iPhones and other Apple products. While Apple does not publish detailed sales data by country, Greater China is the company's third-largest source of revenue ($68.4 billion), according to Apple's 202110-K filings. In 2017, to comply with provisions in China's Cybersecurity Law that require local storage of data generated by Chinese users, Apple announced that it would build a new data center in an area of Guizhou where local authorities offered state support for the construction of data centers operated by domestic technology champions such as Huawei and Tencent, as well as joint ventures with multinational firms including Qualcomm and SAP. In 2018, Apple's joint venture partner in the Guiyang data center, Guizhou-Cloud Big Data Industry Co., Ltd. (GCBD), formally took over as the operator of all iCloud services in mainland China, with Apple listed as a "third party" in the iCloud terms and conditions displayed on devices in China.

In May 2021, before Apple's Guizhou data center formally began operations, a *New York Times* investigation published details of Apple's cybersecurity and data handling arrangements finding that, in addition to being the primary operator of the data center's on-site hardware, GCBD also had access to all data stored on iCloud services in China "under applicable law." Apple had created new encryption keys to be stored on-site after the Chinese government reportedly would not allow Apple to store the encryption keys in the United States as the company has historically done. Although Apple has stated that it maintains control over the encryption keys, several experts have expressed concerns that keeping the encryption keys in China allows Chinese authorities to use the domestic legal system to compel Apple to hand over iCloud user data in cases, rather than use the U.S. court system.

Several human rights experts have pointed to Apple's compliance with China's data governance regime as potentially empowering the Chinese government to exert further control over the global flow of data and information. For example, Apple cited its need to comply with Chinese law following its decision to remove all apps providing VPN services from its App Store in China in 2017 and again, in 2019, when it removed several apps from its Hong Kong App Store that used by protestors in Hong Kong. In response to concerns regarding Apple's business in China and its potential human rights implications, Apple CEO Tim Cook stated that Apple has a "responsibility" to do business in China and that Apple has had to " ... acknowledge that there are different laws in other markets."

Sources: Apple, Inc, "Form 10-K Annual Report Pursuant to Section 13 OR 15(d) of the Securities Exchange Act of 1934 For the fiscal year ended September 25, 2021,"; Sofia Baruzzi, "Guizhou: Investing in China's Big Data Valley and its Sustainable Development," China Briefing, February 26, 2021; Li Tao, "Qualcomm said to end chip partnership with local government in China's rural Guizhou province," *South China Morning Post*, April 19, 2019; Dou Shicong, "Guizhou-Cloud Big Data Takes Over iCloud in China's Mainland," Yicai Global, February 28, 2018; Apple, "iCloud operated by GCBD Terms and Conditions," available at https://www.apple.com/legal/internet-services/icloud/en/gcbd-terms.html; Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," *New York Times*, May 17, 2021; Stephen Nellis and Cate Cadell, "Apple moves to store iCloud keys in China, raising human rights fears," Reuters, February 24, 2018; Associated Press, "Tim Cook defends Apple's pulling of Hong Kong protest App," *Los Angeles Times*, October 10, 2019; Cate Cadell, "Apple says it is removing VPN services from China App Store," Reuters, July 29, 2017; Associated Press, "Tim Cook defends Apple's pulling of Hong Kong protest App," *Los Angeles Times*, October 10, 2019; Cate Cadell, "Apple says it is removing VPN services from China App Store," Reuters, July 29, 2017; and Katie Canales, "Tim Cook says Apple has a 'responsibility' to do business everywhere, even in China despite human rights issues," *Business Insider*, November 10, 2021.

[191] Emphasis added by CRS. Tim Stratford, Eric Carlson, Grace Chen, and Yan Luo, "China Enacts New National Security Law," July 2, 2015, https://www.cov.com/~/media/files/corporate/publications/2015/06/china_passes_new_national_security_law.pdf; full translation of the law available at https://www.chinalawtranslate.com/en/2015nsl/.

In addition to these new laws, which provide an overarching legal framework for further regulation of China's digital economy, the Chinese government has also initiated an aggressive push to formulate national cybersecurity and encryption standards that could pose significant challenges to foreign firms seeking to operate in China. Several business groups in China have expressed concerns that China's process for setting national standards does not sufficiently include input from foreign companies, and that many Chinese national standards do not comply with China's commitments under the WTO Agreement on Technical Barriers to Trade.[192] Some analysts note that the Chinese government has sought to avoid issues in the WTO by downgrading "required" standards to "recommended" standards, but contend that meeting many "recommended" standards is essentially required for multinational firms to compete in China's market.[193]

U.S. Efforts to Address Digital Trade Barriers and IP Theft Issues in China

China's barriers to digital trade not only limit access to China's market for multinational digital services companies, but also serve as a point of leverage to coerce U.S. firms to transfer intellectual property, sensitive technology, and trade secrets to China in order to access its market. As noted earlier, China is considered by many experts to be the largest source of global theft of IP via illicit means and a major source of cyber theft of U.S. trade secrets, including by government entities.[194] Persistent concerns over China's overall policies on IP, technology, and innovation policies led the Trump Administration, in August 2017, to launch a Section 301 investigation of China's trade practices, particularly those considered to facilitate IP theft and technology transfer.[195] On March 22, 2018, President Trump signed a Memorandum on Actions by the United States Related to the Section 301 Investigation that identified four broad IPR-related policies that justified U.S. action under Section 301.[196] At the time, USTR estimated such policies cost the U.S. economy at least $50 billion annually.

The Section 301 findings resulted in a series of increased U.S. tariffs being applied to imports from China and the Chinese government taking similar action on certain U.S. imports in response as retaliatory action. These actions were paused in January 2020 when the United States and China signed a "Phase One" Trade Agreement. [197] Many analysts noted that the Phase One language on intellectual property lacks concrete steps and commitments from China that address its use of regulatory and licensing barriers to limit market access and facilitate tech transfer,

---

[192] Jack Kamensky, "Standards Setting in China: Challenges and Best Practices," *U.S.-China Business Council,* February 2020, https://www.uschina.org/sites/default/files/ standards_setting_in_china_challenges_and_best_practices.pdf; Office of the United States Trade Representative, *2021 National Trade Estimate Report on Foreign Trade Barriers*, March 2021 (Washington, DC), p. 105.

[193] Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business," *Center for Strategic and International Studies*, August 2, 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[194] James Andrew Lewis, "How Much Have the Chinese Actually Taken?" *Center for Strategic and International Studies,* March 22, 2018, https://www.csis.org/analysis/how-much-have-chinese-actually-taken; Center for a New American Security, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," December 2019, p. 24.

[195] For more information on Section 301 of the Trade Act of 1974, see CRS Report R46604, *Section 301 of the Trade Act of 1974: Origin, Evolution, and Use*, by Andres B. Schwarzenberg.

[196] Available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/; For more on executive actions related to the 2018 Section 301 investigation, see CRS In Focus IF11346, *Section 301 of the Trade Act of 1974*, by Andres B. Schwarzenberg.

[197] For a full breakdown of U.S.-China tariff actions, see CRS Report R45949, *U.S.-China Tariff Actions by the Numbers*, by Brock R. Williams and Keigh E. Hammond.

which was acknowledged by both the United States and China as something to be resolved in "Phase Two" discussions.[198] Such discussions have not yet been initiated, though USTR Katherine Tai announced in an October 2021 speech that the Biden Administration will seek to raise "broader policy concerns with Beijing" as it works to enforce the terms of the Phase One deal.[199]

Some experts have suggested the Biden Administration pursue a digital trade deal with U.S. trade partners in the region, including South Korea, Japan, and other countries in Southeast Asia and Oceania, with provisions potentially based on those in the newest U.S. digital trade agreement with Japan (see "U.S.-Japan Digital Trade Agreement").[200] Some observers contend that a broad, inclusive digital trade agreement could provide the United States with an opportunity to establish robust multilateral standards governing cybersecurity standards, cross-border data transfers, and intellectual property, areas where Beijing is increasingly pushing to promote its own standards.[201] China's moves to join regional digital agreements, however, highlights areas where the country's standards and practices, which align closely with its principle of cyber sovereignty, clash with broader consensus among developed economies on the importance of the free flow of data and other policies related to digital trade.[202]

Digital Trade Provisions in Trade Agreements

As the above analysis of EU and China policies demonstrates, no single set of international rules or disciplines governs key digital trade issues. As digital trade has emerged as an important and growing component of trade flows, it has risen in significance on the U.S. trade policy agenda and that of other countries.

WTO members have been at a stalemate and unable to conclude comprehensive multilateral negotiations for over two decades, due to persistent differences among certain members, including between developed and developing countries. In this context, the multilateral trading regime has not kept pace with the complexities of the digital economy and digital trade is treated unevenly in existing WTO agreements. More recent bilateral and plurilateral deals have started to address digital trade policies and barriers more comprehensively. The use of digital trade provisions in bilateral and plurilateral trade negotiations may help spur interest in the creation of future WTO frameworks that focus on digital trade and provide input for ongoing plurilateral negotiations occurring in the aegis of the WTO (see below).

---

[198] U.S.-China Business Council, "US Industry Priorities for US-China Commercial Relations," December 2020, https://www.uschina.org/sites/default/files/us_industry_priorities_for_us-china_commercial_relations_0.pdf; Heather Timmons and Andrea Shalal, "No 'phase two' U.S.–China deal on the horizon, officials say," *Reuters*, November 24, 2019, https://www.reuters.com/article/us-usa-trade-china-phasetwo/no-phase-two-u-s-china-deal-on-the-horizon-officials-say-idUSKBN1XZ00H.

[199] U.S. Trade Representative, *Remarks As Prepared for Delivery of Ambassador Katherine Tai Outlining the Biden-Harris Administration's "New Approach to the U.S.-China Trade Relationship"*, October 4, 2021.

[200] Peter Martin, Eric Martin, and Saleha Mohsin, "Biden Team Weighs Digital Trade Deal to Counter China in Asia," *Bloomberg*, July 12, 2021, https://www.bloomberg.com/news/articles/2021-07-12/biden-team-weighs-digital-trade-deal-to-counter-china-in-asia.

[201] Linh Tong, "Digital Trade Must be Central to Biden's 'Pivot to Asia'," *The Diplomat*, August 10, 2021, https://thediplomat.com/2021/08/digital-trade-must-be-central-to-bidens-pivot-to-asia/; Chun Han Wang, "China Launches Initiative to Set Data-Security Rules," *Wall Street Journal*, September 8, 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[202] Cissy Zhou, "China applies to join digital trade pact with Singapore and NZ," *Nikkei Asian Review*, November 1, 2021, https://asia.nikkei.com/Economy/Trade/China-applies-to-join-digital-trade-pact-with-Singapore-and-NZ.

WTO Provisions

While no comprehensive agreement on digital trade exists in the WTO, certain WTO agreements and ongoing plurilateral negotiations cover some aspects of digital trade.

General Agreement on Trade in Services (GATS)

The WTO General Agreement on Trade in Services (GATS) entered into force in January 1995, predating the current reach of the internet and explosive growth of global data flows. GATS includes obligations on nondiscrimination and transparency that cover all service sectors. The market access obligations under GATS, however, are on a "positive list" basis in which each party must specifically opt in for a given service sector to be covered.[203]

As GATS does not distinguish between means of delivery, trade in services via electronic means is covered under GATS. Some WTO observers have referred to the need for a new mode of service within GATS to better capture services that are embedded in goods, many of which rely on digital technologies (e.g., software in mobile phones, motor vehicles built-in voice assistant, or IoT tracking devices), with the aim of separating out such services to create an opportunity for further trade liberalization and acceleration of the digital economy.[204]

While GATS contains explicit commitments for telecommunications and financial services that underlie e-commerce, barriers on digital trade and information flows, for example, are not specifically included. Given the positive list approach of GATS, coverage across members varies and many newer digital products and services did not exist when the agreements were negotiated. To address advances in technology and services, the Committee on Specific Commitments is examining how certain new online services, such as platform services, or specific regulations, such as data localization, could be classified and scheduled within GATS.[205] Some analysts have suggested forming a new Committee on Digital Services Trade for a dedicated dialogue on digital services issues and best practices.[206]

Declaration on Global Electronic Commerce

In May 1998, WTO members established the "comprehensive" Work Programme on Electronic Commerce to examine trade-related issues relating to global e-commerce. Recent discussions include examining the COVID-19 pandemic's impact on e-commerce, including the implications for cross-border trade.[207]

When creating the Work Programme, WTO members established a temporary customs duties moratorium on electronic transmission that has been extended multiple times.[208] While members agreed to extend the moratorium until the 12th Ministerial Conference planned for November 2021, its future is unclear. One issue is that members disagree over what is covered by electronic

[203] For more information, see https://www.wto.org/english/tratop_e/serv_e/serv_e.htm, and CRS Report R43291, *U.S. Trade in Services: Trends and Policy Issues*, by Rachel F. Fefer.

[204] Alessandro Antimiani and Lucian Cernat, "Liberalizing Global Trade in Mode 5 Services: How Much is it Worth," DG TRADE, European Commission, July 2017.

[205] World Trade Organization, "WTO members hold latest "cluster" of services meetings," March 21, 2019.

[206] Erik van der Marel, "Lessons from the pandemic for trade cooperation in digital services," European Centre for International Political Economy, November, 2011.

[207] WTO, "WTO report looks at role of e-commerce during the COVID-19 pandemic," May 4, 2020.

[208] For more information, see https://www.wto.org/english/tratop_e/ecom_e/ecom_briefnote_e.htm.

transmissions. India and South Africa, in particular, are seeking to amend the moratorium to narrow its scope, arguing that they are giving up a potential revenue stream. The countries cite a United Nations (UN) report advocating for an end to the moratorium because, as increasing volumes of electronic transmissions replace trade in physical goods, governments are losing out in the form of foregone tariffs, as much as $3.4 billion for developing countries.[209] In contrast, an OECD study found that foregone revenue of the moratorium is likely to be relatively small and that its lapse would come at the expense of wider gains in the economy including export competitiveness and productivity.[210] Another study specifically questions the U.N. research methodology and calculates that a country would lose considerably more in GDP than they would gain in tariff revenue.[211]

Information Technology Agreement (ITA)

The WTO Information Technology Agreement (ITA) aims to eliminate tariffs on the goods that power and utilize the internet, lowering the costs for companies to access technology at all points along the value chain. Originally concluded in 1996, the ITA was expanded to further cut tariffs beginning in July 2016. Like the original agreement, the expanded ITA is a plurilateral agreement among over 50 developed and developing WTO members who account for over 90% of global trade in these goods. Some WTO members, such as Vietnam and India, are party to the original plurilateral ITA, but did not join the expanded agreement. Like the original ITA, the benefits of the expanded agreement will be extended on a most-favored nation (MFN) basis to all WTO members.

Under the expanded ITA, the parties agreed to review the agreement's scope in the future to determine if additional product coverage is warranted as technology evolves. Some observers have advocated for further expanding the list to take into account many of the medical technologies needed during the COVID-19 pandemic. While the WTO ITA has expanded trade in the technology products that underlie digital trade, it does not tackle the nontariff barriers that can pose significant limitations.

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)

The TRIPS Agreement, in effect since January 1, 1995, provides minimum standards of IPR protection and enforcement for WTO members. Much of the negotiations leading to TRIPS date to the 1980s, before the Internet age and the agreement is not specifically focused on IPR issues in the digital environment.[212]

TRIPS covers copyrights and related rights (i.e., for performers, producers of sound recordings, and broadcasting organizations), trademarks, patents, trade secrets (as part of the category of "undisclosed information"), and other forms of IP. It builds on international IPR treaties, dating to the 1800s, administered by the World Intellectual Property Organization, or WIPO (see below).

---

[209] Rashmi Banga, "Growing Trade in Electronic Transmissions: Implications for the SouthUNCTAD Research Paper No. 29," UNCTAD/SER.RP/2019/1.

[210] Andrenelli, A. and J. López González (2019), "Electronic transmissions and international trade—shedding new light on the moratorium debate", OECD Trade Policy Papers, No. 233, OECD Publishing, Paris, https://doi.org/10.1787/57b50a4b-en.

[211] Hosuk Lee-Makiyama, "The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions," European Centre for International Political Economy, August 1, 2019.

[212] Wolf R. Meier-Ewert and Jorge Gutierrez, "Intellectual Property and Digital Trade—Mapping International Regulatory Responses to Emerging Issues," WTO, Staff Working Paper, February 3, 2021. For background, see CRS Report RL34292, *Intellectual Property Rights and International Trade*, by Shayerah I. Akhtar, Ian F. Fergusson, and Liana Wong.

TRIPS incorporates the main substantive provisions of WIPO conventions by reference, making them obligations under TRIPS. Most WTO members were required to fully implement TRIPS by 1996, with transition periods for developing country members (until 2000) and least-developed-country (LDC) members (until July 1, 2034).

TRIPS aims to balance the rights and obligations between protecting private rights holders' interests and securing broader public benefits. Among its provisions, the TRIPS section on copyright and related rights includes specific provisions on computer programs and compilations of data. It requires protections for computer programs—whether in source or object code—as literary works under the WIPO Berne Convention for the Protection of Literary and Artistic Works (Berne Convention). TRIPS also clarifies that databases and other compilations of data or other material, whether in machine-readable form or not, are eligible for copyright protection even when the databases include data not under copyright protection.[213] TRIPS provisions have set a foundation for IPR provisions in subsequent U.S. trade negotiations and agreements, many of which are "TRIPS-plus."

Like the GATS, TRIPS predates the era of ubiquitous internet access and commercially significant e-commerce. TRIPS includes a provision for WTO members to "undertake reviews in the light of any relevant new developments which might warrant modification or amendment" of the agreement. The TRIPS Council previously engaged in discussions on the agreement's relationship to electronic commerce as part of the WTO Work Programme on Electronic Commerce, focusing on copyright and related rights, trademarks, and new technologies.

World Intellectual Property Organization (WIPO) Internet Treaties

The World Intellectual Property Organization (WIPO) has been a primary forum to address IP issues brought on by the digital environment since the TRIPS Agreement. The 1996 WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) established international norms regarding IPR protection in the digital environment. Known as "the WIPO Internet Treaties," they include provisions for legal protection and remedies against circumventing technological protection measures (TPMs), such as encryption, and against the removal or alteration of rights management information (RMI), which is data identifying works or their authors necessary for them to manage their rights (e.g., for licenses and royalties). A contested issue in WIPO negotiations was treatment of the liability of online service providers and other communication entities that provide access to the internet. In the end, WIPO Internet Treaties leave it to the discretion of national governments to develop the legal parameters for ISP liability.[214] According to USTR, these treaties "have raised the standard of copyright protection around the world, particularly with regard to online delivery of copyrighted content."[215] While the WIPO Internet Treaties have some provisions that are similar to and build on TRIPS, obligations under them currently are not subject to WTO dispute resolution.[216]

---

[213] WTO, "Overview: The TRIPS Agreement," https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm. For more information, see CRS Report RL34292, *Intellectual Property Rights and International Trade*, by Shayerah Ilias Akhtar and Ian F. Fergusson.

[214] U.S. Congress, Senate Committee on Foreign Relations, *WIPO Copyright Treaty (WCT) (1996) and WIPO Performances and Phonograms Treaty (1996)*, Report to accompany treaty document 105-17, 105th Cong., 2nd sess., October 14, 1998, S.Exec. Rept. 105-25.

[215] USTR, *2021 Special 301 Report*, April 2021, p. 11.

[216] WIPO, "The Advantages of Adherence to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)," p. 10, available at https://www.wipo.int/export/sites/www/copyright/en/activities/pdf/advantages_wct_wppt.pdf.

As of November 2021, the WCT had 110 contracting parties, and WPPT had 109 contracting parties. The United States implemented the WIPO Internet Treaties through the Digital Millennium Copyright Act of 1998 (DMCA) (P.L. 105-304), which included new standards for protecting and enforcing copyrights in the digital environment, and certain "safe harbors" from copyright infringement liability for ISPs.[217] India was one of the latest countries to join the treaties, entering them into force on December 25, 2018. The United States continues to call on trading partners to fully implement the WIPO Internet Treaties.

Certain U.S. FTAs, including the U.S.-Mexico-Canada Agreement (USMCA, see below), as well as other countries' trade agreements, make reference to WIPO Internet Treaties, such as by reaffirming or requiring compliance with them. IP and digital trade present a number of potential issues regarding WIPO. Some stakeholders and analysts, for instance, have questioned whether the TRIPS Agreement should incorporate the WIPO Internet Treaties, as it did with certain other WIPO treaties.[218] Additional issues which WIPO is exploring include artificial intelligence and whether existing IP frameworks should be modified for machine-created inventions and works. Areas of inquiry include potential protection for the actual machine-created work, AI algorithms and software, and the underlying training data and data inputs.[219]

Current WTO Plurilateral Negotiations

At the WTO over 80 other parties are participating in ongoing negotiations on e-commerce aiming to establish a global framework and obligations that enable digital trade in a nondiscriminatory and less trade restrictive manner. Australia, Japan, and Singapore are the co-conveners of the Joint Statement Initiative (JSI) on E-commerce, and participants include United States, the EU, and also several developing countries, such as China and Brazil. India stated it will not join, preferring to maintain its flexibility to favor domestic firms, limit foreign market access, and raise revenue in the future through potential customs duties.[220] In addition, India and South Africa are actively challenging the legal status of the "Joint Statement Initiative" negotiations because they are not being conducted on a multilateral basis.[221]

The initial U.S. proposal for the negotiations is based on the USMCA Digital Trade chapter and U.S.-Japan Digital Trade Agreement (see below). The U.S. objectives for a high standard

[217] For more information on this statute, see CRS Report R43436, *Safe Harbor for Online Service Providers Under Section 512(c) of the Digital Millennium Copyright Act*, by Brian T. Yeh.

[218] TRIPS incorporates by reference all of the substantive obligations of the Paris Convention for the Protection of Industrial Property (adopted in 1883 and applying to industrial property "in the widest sense," including patents, trademarks, industrial designs, and geographical indications) and the Berne Convention for the Protection of Literary and Artistic Works (adopted in 1886 and applying to copyrights and related rights), save for the Berne Convention's provisions on moral rights. TRIPS also uses provisions of some other IPR-related international agreements. See WIPO, "WIPO-Administered Treaties," available at https://www.wipo.int/treaties/en/; and WTO, "What is the Relationship Between the TRIPS Agreement and the Pre-existing International Conventions that it Refers to?," available at https://www.wto.org/english/tratop_e/trips_e/tripfq_e.htm#TripsAndConventions.

[219] WIPO, "WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI), Second Session," May 21, 2020.

[220] Subhayan Chakraborty, "India refuses to join e-commerce talks at WTO, says rules to hurt country," *The Business Standard*, February 25, 2019.

[221] India and South Africa submission to the WTO General Council, "The Legal Status of "Joint Statement Initiatives" and Their Negotiated Outcomes," WT/GC/W/819, February 19, 2021.

agreement include market access, data flows, nondiscriminatory treatment of digital products, protection of IP and digital security measures, and intermediary liability, among others.[222]

The co-conveners aim to have ten areas of "clean text" before the Ministerial Conference in November 2021, which has now been postponed until next year at a date to be determined due to the Covid-19 pandemic. As of September, the parties had finalized text on unsolicited messages (spam), electronic signatures and authentication, e-contracts, open government data and, online consumer protection.[223] Other areas remain contentious. For example, the United States and the EU have similar positions on many issues. The EU's strict rules on data privacy impose more constraints on cross-border data flows compared to U.S. laws, making it unclear if the two sides will be able to reconcile their different regulatory approaches to create common rules. Additionally, with regard to data flows and data storage, China has proposed the negotiations be limited to exploratory discussions rather than establishing obligations and has generally supported nonbinding standards.[224]

The outlook may be challenging given the different approaches and policies, especially among the United States, the EU, and China. Some analysts believe that the plurilateral WTO negotiators will have to decide between scope and depth to reach a final agreement. A narrow agreement with limited scope and provisions would likely retain the greatest number of negotiating participants, including China, but could have less impact on eliminating barriers to and establishing nondiscriminatory rules and disciplines in digital trade if it does not address contentious issues such as data flows or emerging technologies. On the other hand, a higher-standard agreement with deeper and potentially more impactful commitments, whether on privacy or online content moderation, may deter participants who are not willing or able to accept the obligations. There is no agreement on whether the final obligations will be subject to dispute settlement, which will affect the potential enforceability of the scope and depth of commitments agreed upon among participants. Lesser-developed countries' support may be linked to capacity building and technical assistance, in addition to other flexibilities.

U.S. Bilateral and Plurilateral Agreements

As data is increasingly incorporated into international trade, the line between goods and services, and the application of existing multilateral trade agreement rules and disciplines, is not always clear. As discussed above, WTO agreements provide limited treatment of some aspects of digital trade. One study of preferential trade agreements (PTAs) show that most PTAs also fall short of comprehensively addressing what it deems are the five pillars of digital trade integration: reducing digital trade barriers, digital trade facilitation, digital trade regulatory frameworks and digital trust policies, digital development and inclusion, and institutional coordination.[225] Part of the challenge is that, unless updated, trade agreement provisions on digital trade can quickly become outdated as new technology challenges or types of barriers emerge that were unforeseen.

The United States has sought to remove trade barriers to and establish new rules and disciplines on digital trade in its bilateral and plurilateral trade negotiations. The United States has included

[222] The United States, "Joint Statement on Electronic Commerce Initiative," WTO, April 12, 2018.

[223] WTO, "E-commerce talks: two "foundational" articles cleaned; development issues discussed," press release, September 13, 2021.

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

[225] Andrew D. Mitchell and Neha Mishra, *Digital trade integration in preferential trade agreements*, ARTNeT, AWP 191, May 2020, https://artnet.unescap.org/publications/working-papers/digital-trade-integration-preferential-trade-agreements.

an e-commerce chapter in its FTAs since it signed an agreement with Singapore in 2003.[226] The e-commerce chapter of U.S. FTAs, which have evolved over time, usually begins by recognizing e-commerce as an economic driver and the importance of removing trade barriers to e-commerce.[227] Most chapters contain provisions on nondiscrimination of trade in digital products, prohibition of customs duties, transparency, and cooperation mechanisms on topics such as SMEs, consumer protection, cross-border information flows, and promoting dialogues to develop e-commerce. All FTAs allow certain exceptions to ensure that each party is able to protect regulatory flexibility to achieve legitimate public policy objectives.

United States-Mexico-Canada Agreement (USMCA)

The 1994 North American Free Trade Agreement (NAFTA), among the United States, Mexico, and Canada, was negotiated before the internet age and did not contain provisions to address digital trade. Under the USMCA, which updated and replaced NAFTA, the parties agreed to a common set of digital trade rules. USMCA entered into force on July 1, 2020.[228]

USMCA is the first approved U.S. FTA with broad commitments on digital trade, and its provisions are generally subject to USMCA dispute settlement procedures.[229] In addition to specific obligations (see **text box**), the USMCA encourages cooperation between the parties on specific issues related to data privacy and security, interoperability, self-regulation by the private sector, and small and mid-size enterprises (SMEs).

Selected Provisions of USMCA

- **Customs duties and nondiscrimination.** Generally prohibits customs duties on products transmitted electronically and also prohibits discrimination against digital products, including coverage of certain tax measures.
- **Digital trade facilitation**. Permits use of electronic authentication and signatures, electronic payment systems, and consumer access to the internet, and requires anti-spam measures.
- **Cross-border data flows and data localization.** Prohibits restrictions on cross-border data flows, except as necessary for "legitimate public policy objectives," and prohibits requirements for "localization of computing facilities" (i.e., data localization) as a condition for conducting business. In the financial services chapter of the agreement, data localization requirements are prohibited, as long as financial regulators have access to information for regulatory and supervisory purposes.
- **Consumer protection and privacy.** Requires parties to adopt or maintain online consumer protection laws, as well as a legal framework to protect the personal information of users of digital trade. The content and enforcement of these laws are left to each government's discretion, but the provision identifies specific key principles and Asia-Pacific Economic Cooperation (APEC) and OECD guidelines that the parties must take into account in developing their framework. The parties also agree to further develop and promote interoperability systems between privacy regimes, including the APEC Cross-Border Privacy Rules (CBPR) system of which all three countries are members (see below).
- **Source code and technology transfer.** Prohibits requiring the transfer or disclosure of software source code or algorithms as a condition for market access, with some exceptions.

[226] https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf.

[227] This statement was used in U.S. free trade agreements with Australia, Bahrain, Colombia, Central America and the Dominican Republic, Morocco, Oman, Panama, Peru, and South Korea. Chile used a slightly different text.

[228] For more on USMCA, see CRS Report R44981, *The United States-Mexico-Canada Agreement (USMCA)*, by M. Angeles Villarreal and Ian F. Fergusson.

[229] The Obama Administration negotiated enforceable digital trade commitments as part of the Trans-Pacific Partnership (TPP), which became the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP/TPP-11) following the U.S. withdrawal from TPP in 2017. While the CPTPP retains the commitments negotiated under the TPP, the CPTPP also contains certain country-specific exemptions through side letters to the agreement, some of which affect digital trade commitments. USMCA builds on TPP commitments.

- **Liability for interactive computer services.** Limits imposing civil liability with respect to third-party content for internet platforms that depend on interaction with users, with some exclusions such as for intellectual property rights infringement.
- **Cybersecurity.** Commitments promote collaboration and use of risk-based strategies and consensus-based standards over prescriptive regulation in dealing with cybersecurity risks and events.
- **Cryptography.** Commitments prohibit requiring the transfer or access to proprietary information, including a particular technology or production process, by manufacturers or suppliers of information and communication technology (ICT) goods that use cryptography, as a condition for market access, with some exceptions, such as for networks and devices owned, controlled, or used by government.
- **Dispute settlement**. Commitments may be enforced through the through consultation and/or additional formal dispute settlement procedures.

Sources: Drawn from the relevant sections of the USMCA text, including the Digital Trade chapter available at: USMCA, Chapter 19, "Digital Trade," at https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf and sectoral annexes at https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/12_Sectoral_Annexes.pdf.

The digital trade chapter garnered overall support from U.S. stakeholders.[230] However, one area of controversy that emerged is the chapter's prohibition of liability of internet intermediaries, which reflects current U.S. law in Section 230 of the Communications Decency Act of 1996.[231] Some lawmakers have expressed concerns about including the Section 230 liability shield in trade agreements, and some Members seek to change the scope of, or otherwise make amendments, to the immunity protection in U.S. law.[232] Lawmakers also have raised similar concerns regarding the digital agreement with Japan (see below).

U.S.-Japan Digital Trade Agreement

The U.S.-Japan Digital Trade Agreement, which entered into force in January 2020, as an executive agreement, was negotiated by the Trump Administration as "stage one" of broader prospective trade talks with Japan.[233] Former USTR Robert Lighthizer referred to the U.S.-Japan agreement, which parallels USMCA digital trade provisions, as the "most comprehensive and high-standard trade agreement" negotiated on digital trade barriers.[234]

Commitments in the U.S.-Japan Digital Trade Agreement broadly reflect those in USMCA, but diverge in some areas. For example, the agreement excludes the explicit reference to APEC or OECD privacy frameworks and incorporates provisions on cryptography in a sectoral annex, as opposed to the digital trade chapter of USMCA, and does not subject its commitments to dispute settlement unlike the USMCA.

[230] For example, see Coalition of Services Industries (CSI) statement on Senate Passage of the USMCA Implementing Bill, January 16, 2020; Anupam Chander, "The Coming North American Digital Trade Zone," Council on Foreign Relations, October 9, 2018; and Michael Beckerman, "Passing USMCA will help US companies address global threats to digital trade," *The Hill*, January 10, 2020.

[231] For more information on Section 230 of the Communications Decency Act, see CRS Report R46751, *Section 230: An Overview*, by Valerie C. Brannon and Eric N. Holmes.

[232] Lauren Feiner, "Pelosi pushes to keep tech's legal shield out of trade agreement with Mexico and Canada," *CNBC*, December 5, 2019.

[233] For more detail, see CRS Report R46140, *"Stage One" U.S.-Japan Trade Agreements*, coordinated by Brock R. Williams. For the text of the agreement, see https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text.

[234] USTR, "FACTSHEET on U.S.-Japan Digital Trade Agreement," October 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement.

Other International Forums for Digital Trade

While U.S. and international trade agreements are one way for the United States to establish market opening and new rules and disciplines to govern digital trade, not every issue is necessarily suitable for an international trade agreement and not every international partner may be ready, or willing, to take on such commitments or may take a different view on the appropriate digital trade rules. In such cases, the United States and other countries may pursue other approaches to encourage high-level, nonbinding best practices and principles and align expectations.

G-7. The influential Group of Seven (G-7) is one venue for establishing common principles, and digital issues have been on its agenda recently.[235] At the October 2021 meeting of G-7Trade Ministers, the parties adopted the G-7 Digital Trade Principles, committing to open digital markets; data free flow with trust; safeguards for workers, consumers, and businesses; digital trading systems; and fair and inclusive global governance.[236] Provisions in the agreement oppose digital protectionism and authoritarianism, endorse the WTO moratorium on customs duties, promote interoperability and digitization, and support efforts to tackle the digital divide, among others. The Principles build on the April 2021 Digital and Trade Ministerial meeting by G-7 nations that resulted in a framework for collaboration on digital standards, a roadmap for cooperation on data free flow with trust, and plans to work with OECD and other ongoing global initiatives and multi-stakeholder dialogues to share best practices, build regulatory cooperation, and support international standards and norms.[237]

OECD. The OECD provides a forum to discuss principles and norms to facilitate a thriving digital economy. The United States could work with its OECD partners to reinforce principles, including an open internet and how best to balance public policy objectives. For example, the United States has endorsed the OECD Principles on Artificial Intelligence that promote AI that is "innovative and trustworthy and that respects human rights and democratic values."[238] An ongoing OECD initiative is to develop general principles for enhancing access to and sharing data across the economy coherently and in alignment with OECD guidance and best practices on issues such as data openness, transparency, stakeholder engagement, IPR, and pricing. As noted earlier, the OECD served as a venue for negotiations between the United States and over 130 other countries on a multilateral, consensus-based solution to the tax challenges arising from the digitalization of the global economy.[239]

APEC. The APEC forum presents an opportunity for sharing best practices and setting high-level principles on issues that may be of greater concern to developing countries with less advanced

[235] The Group of Twenty (G-20) is a forum for advancing international cooperation and coordination among 20 major advanced and emerging-market economies. The G-20 includes Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, United Kingdom, and the United States, as well as the European Union (EU). See CRS Report R40977, *International Economic Policy Coordination at the G-7 and the G-20*, by Rebecca M. Nelson.

[236] UK Department for International Trade, "G7 Trade Ministers' Digital Trade Principles," October 22, 2021.

[237] For more information, please see UK Department for Digital, Culture, Media & Sport, "G7 Digital and Technology—Ministerial Declaration," *Notice*, April 28, 2021, https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration.

[238] U.S. Mission to the Organization For Economic Cooperation & Development, *Michael Kratsios, Deputy Assistant to the President for Technology Policy OECD Forum and Ministerial Council Meeting*, May 21, 2019. For more information, see https://www.oecd.org/going-digital/ai/principles/.

[239] For more information, see OECD Tax Talks, https://www.oecd.org/tax/beps/tax-talks-webcasts.htm.

digital economies and industry.[240] In a 2021 trade meeting, APEC ministers noted the importance of digitalization for economic growth and called for accelerated implementation of related APEC work programs and digitalization of trade facilitation processes to improve border processes and enhance supply chains.[241] Due to its voluntary nature, APEC has served as an incubator for potential future plurilateral agreements (see **text box**).

APEC Cross-Border Privacy Rules (CBPR)

APEC is implementing the Cross-Border Privacy Rules (CBPR) system to be consistent with its existing APEC Privacy Framework. Currently, the United States, Japan, Mexico, Canada, South Korea, Singapore, Taiwan, Philippines, and Australia are CBPR members. According to the Business Software Alliance, most countries have data protection frameworks based on either the APEC CBPR system or the EU regime, but some countries still lack privacy laws. Some observers view CBPR, which aims to reflect a diversity of national privacy regimes, as a scalable solution that could potentially be adopted multilaterally. Others may view the EU regime as a more comprehensive, top-down approach.

Sources: APEC, Enabling Electronic Commerce: The Contribution of APEC's Data Privacy Framework, available at https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group and BSA, Global Cloud Computing Scorecard, 2016 and 2018.

Regulatory cooperation. Ongoing regulatory cooperation efforts are another important tool for addressing differences between parties, better aligning regulatory requirements, and reducing inconsistencies and redundancies that can hamper or discriminate against the free flow of data, goods, and services. These forums provide an opportunity for U.S. agencies to work directly with overseas counterparts and focus on specific aspects of digital trade such as online privacy, consumer protection, and rules for online contract formation and enforcement. The EU-U.S. Privacy Shield is one example of regulatory authorities working together to address such issues.

Issues for Congress

Complex policy issues and questions continue to evolve as the internet-driven economy grows and new innovations emerge. Digital trade is intimately connected to and woven into all parts of the U.S. economy and it overlaps with other sectors, requiring policymakers to balance many different objectives and policy approaches. For example, digital trade relies on cross-border data flows, but policymakers must balance open data flows with public policy goals such as protecting data privacy, supporting law enforcement, and improving personal safety and national security.

The complexity of the debate related to cross-border data flows and digital trade more generally involves complementary and competing interests and stakeholders. Companies and individuals who seek to do business and open markets abroad may focus on maintaining market access, which may include cross-border data flows, while others, such as in import competing sectors, may seek to limit foreign competition. Privacy advocates may focus on protecting personal information, while businesses may seek to use such data to create new innovative products and for options, such as personalization and targeted advertising. Meanwhile, law enforcement and defense advisors may seek the ability to access or limit information flows based on national security interests, such as restricting the ability of certain other actors to obtain, process, or transmit data generated by U.S. citizens. In crafting policy, trade negotiators must balance these competing stakeholder interests and other public policy objectives.

[240] Asia Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 with 21 Asian Pacific economies as members. See http://www.apec.org/About-Us/About-APEC.aspx.

[241] APEC, *APEC Ministers Responsible for Trade Meeting Joint Statement 2021*, Wellington, New Zealand, June 4, 2021, https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Trade/2021_MRT.

Digital trade raises numerous issues of potential oversight and legislative interest to Congress, including the following:

- Understanding the impact of digital trade on the U.S. economy and the effects of localization and other digital trade barriers on U.S. trade and investment, firms and their workers, and competition.
- Examining how to best balance market openness and cross-border data flows with other policy goals, such as the right to privacy and the government's need to access or limit access to certain data to protect safety and national security.
- Considering if the United States would benefit from an overarching digital privacy policy and what possible lessons to draw from other countries' experiences, and how to best balance this with U.S. trade negotiating objectives. Part of this examination could include a comparison of the EU's and China's policies on personal data and the extent to which each may set de facto global standards if other countries copy them in part or in whole. Congress may also consider the potential opportunity for the United States to enhance its role in shaping global data protection standards, especially if it were to adopt more overarching policies.
- Reviewing the U.S. role in standard-setting bodies and how best to ensure pro-active leadership to shape international standards, including to respond to standard-setting practices of other economies that may have global reach or may have aspects that are unduly protectionist and discriminatory. The standard-setting practices of major economies such as China and the EU may be of particular interest.
- Examining evolving U.S. trade policy efforts and how best to achieve commercially meaningful outcomes, whether through ongoing plurilateral negotiations at the WTO or implementation of the OECD digital tax agreement, each of which may set new binding and nonbinding rules and disciplines, or if new approaches are needed to advance U.S. commercial interests.
- Conducting oversight to provide input into ongoing digital discussions with the EU, including negotiations to revise the EU-U.S. Privacy Shield Framework, working groups set up under the new Trade and Technology Council (TTC), and the EU-U.S. Joint Technology Competition Policy Dialogue. Efforts could include a joint examination of key differences between the GDPR and China's new laws and regulations governing cross-border data flows.
- Examining how to work with leading allies, including the EU and Japan, to jointly respond to the challenges posed by China's digital authoritarianism approach and other non-market economy policies, especially with respect to forced technology standards, theft of U.S. IPR, and market access barriers, and whether new legislative authorities are needed to do so more effectively. For example, additional considerations might include placing limits on U.S. firms' involvement in constructing data infrastructure in China that contributes to China's surveillance and control of cross-border data flows, or the introduction of disclosure requirements for firms that share certain categories of data with Chinese authorities.
- Considering whether and how to update the digital trade-related negotiating objectives in potential new TPA legislation, as well as examining the standalone U.S.-Japan Digital Trade Agreement and USMCA digital trade provisions and

- whether they should serve as a model to address digital trade in broader FTAs. Part of this examination could include which enforcement mechanisms may be best suited for obligations on digital trade in potential future FTAs.
- Conducting oversight into whether the United States should pursue a digital trade agreement with Indo-Pacific partners to shape global standards and counter China's growing interest in shaping norms and standards governing digital trade or whether the United States should consider joining, and potentially revising, existing regional agreements. This oversight may entail a closer examination of the key differences and costs and benefits of cooperative approaches, as compared to enforceable commitments.

Author Information

Rachel F. Fefer, Coordinator
Analyst in International Trade and Finance

Michael D. Sutherland
Analyst in International Trade and Finance

Shayerah I. Akhtar
Specialist in International Trade and Finance

Acknowledgments

Special acknowledgement to Amber Wilhelm, Edward Gracia, Jennifer Roscoe, and Paulo Ordoveza for creation of the graphics.

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.