Congressional Research Service
Informing the legislative debate since 1914

Digital Trade and U.S. Trade Policy

May 21, 2019

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

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

As the global internet develops and evolves, digital trade has become more prominent on the global trade and economic policy agenda. The economic impact of the internet was estimated to be $4.2 trillion in 2016, making it the equivalent of the fifth-largest national economy. The digital economy accounted for 6.9% of current-dollar gross U.S. domestic product (GDP) in 2017. Digital trade has been growing faster than traditional trade in goods and services.

Congress has an important role to play in shaping global digital trade policy, from oversight of agencies charged with regulating cross-border data flows to shaping and considering legislation implementing new trade rules and disciplines through trade negotiations. Congress also works with the executive branch to identify the right balance between digital trade 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 productivity-enhancing tools like cloud data storage and email. In 2017, U.S. exports of information and communications technology-enabled services (excluding digital goods) were an estimated $439 billion. Digital trade is growing on a global basis, contributing more to global domestic product (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, in particular, such as those on internet sovereignty and cybersecurity, pose challenges for U.S. companies.

Digital trade issues often overlap and cut across policy areas, such as IPR and national security; this raises questions for Congress as it weighs 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), other 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 proposed U.S.-Mexico-Canada Agreement (USMCA) and ongoing plurilateral discussions in the WTO on a potential e-commerce agreement could address digital trade barriers to varying degrees. Digital trade is also being discussed in a variety of international forums, providing the United States with multiple opportunities to engage in and shape global norms.

With workers in the high-tech sector in every U.S. state and congressional district, and 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. interests.

Contents

Introduction 1
Role of Digital Trade in the U.S. and Global Economy 2
Economic Impact of Digital Trade 5
Digitization Challenges 8
Digital Trade Policy and Barriers 10
Tariff Barriers 12
Nontariff Barriers 13
Localization Requirements 13
Intellectual Property Rights (IPR) Infringement 15
National Standards and Burdensome Conformity Assessment 17
Filtering, Blocking, and Net Neutrality 18
Cybersecurity Risks 18
U.S. Digital Trade with Key Trading Partners 20
European Union 20
EU-U.S. Privacy Shield 22
General Data Protection Regulation (GDPR) 23
Digital Single Market (DSM) 23
China 24
Internet Governance and the Concept of "Internet Sovereignty" 26
Cyber-Theft of U.S. Trade Secrets 26
Cybersecurity Laws 28
Section 301 Action against China over Intellectual Property and Innovation Issues 29
Digital Trade Provisions in Trade Agreements 31
WTO Provisions 31
General Agreement on Trade in Services (GATS) 32
Declaration on Global Electronic Commerce 32
Information Technology Agreement (ITA) 32
Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 32
World Intellectual Property Organization (WIPO) Internet Treaties 33
WTO Plurilateral Effort 34
U.S. Bilateral and Plurilateral Agreements 35
Existing U.S. Free Trade Agreements (FTAs) 35
United States-Mexico-Canada Agreement (USMCA) 36
Other International Forums for Digital Trade 36
Issues for Congress 38

Figures

Figure 1. Effect on World GDP (percent) 2
Figure 2. Snapshot of Most Popular Websites 3
Figure 3. What is Digital Trade? 5
Figure 4. Select U.S.-EU Cross-Border E-Commerce Purchases 20
Figure 5. Digitally Deliverable Service Exports 2017 21
Figure 6. Digitally Deliverable Services Incorporated into Global Value Chains 21

Figure 7. The U.S. and China Digital Trade Markets 24
Figure 8. Three Rounds of U.S.-China Tariff Hikes in 2018 31

Figure A-1. Levels of Perceived Digital Trade Barriers in Selected Countries 40

Tables

Table 1. AmCham China Business Survey: Percent of Respondents who said Certain Chinese IT Policies Affected their Operations and Competitiveness in China Somewhat or Severely 25

Appendixes

Appendix. Digital Trade Barriers 39

Contacts

Author Information 41
Acknowledgments 41

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 6.9% of U.S. GDP in 2017, including (1) information and communications technologies (ICT) sector and underlying infrastructure, (2) digital transactions or e-commerce, and (3) digital content or media.[1] The digital economy supported 5.1 million jobs, or 3.3% of total U.S. employment in 2017, and almost two-thirds of jobs created in the United States since 2010 required medium or advanced levels of digital skills.[2] 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 follows:

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

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 infringement of intellectual property rights (IPR) or protective industrial policies, often overlap and cut across sectors. In some cases, policymakers may struggle to balance digital trade objectives with other legitimate policy issues related to 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, and an increasing number of cybertheft incidents that have affected U.S. consumers and companies. These concerns may raise the general U.S. interest in promoting, or restricting, cross-border data flows and in enforcing compliance with existing rules. Congress has an interest in ensuring the global rules and norms of the internet economy are in line with U.S. laws and norms.

Trade negotiators continue to explore ways to address evolving digital issues in trade agreements, including in the proposed U.S.-Mexico-Canada Agreement (USMCA). Congress has an important role in shaping digital trade policy, including oversight of 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.

---

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

[2] Penny Pritzker and John Engler, Director Edward Alden, *The Work Ahead: Machines, Skills, and U.S. Leadership in the Twenty-First Century, Independent Task Force Report*, The Council for Foreign Relations, April 2018.

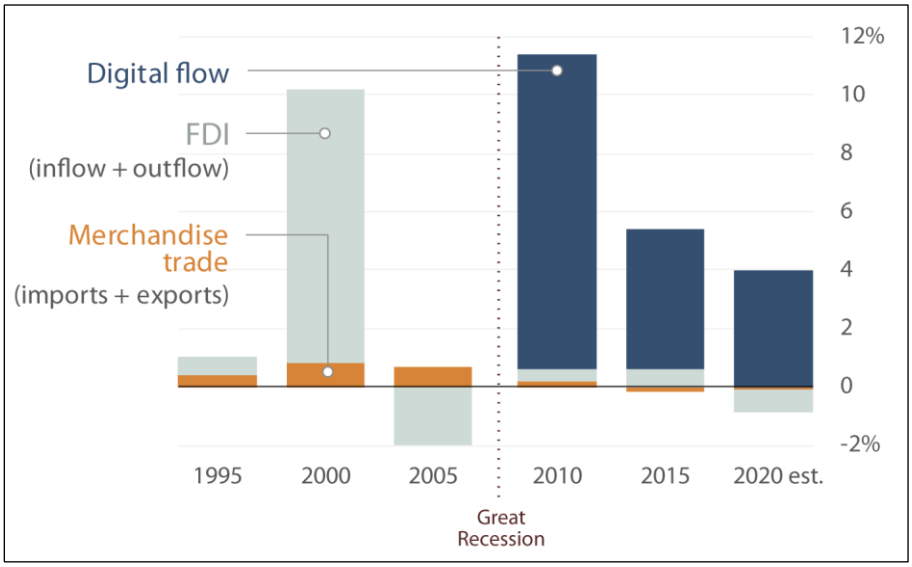
[3] Ibid. and U.S. International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, p.33, https://www.usitc.gov/publications/332/pub4716.pdf.

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 U.S. and Global Economy

The internet is not only a facilitator of 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. According to one estimate, the volume of global data flows (sending of digital data such as from streaming video, monitoring machine operations, sending communications) is growing faster than trade or financial flows. One analysis forecasts the global flows of goods, foreign direct investment (FDI), and digital data will add 3.1% to gross domestic product (GDP) from 2015-2020. The volume of global data flows is growing faster than trade or financial flows, and its positive GDP contribution offsets the lower growth rates of trade and FDI (see **Figure 1**).[4] Focusing domestically, the Bureau of Economic Analysis (BEA) estimates that, from 1997-2017, real value added for the digital economy outpaced overall growth in the economy each year and, in 2017, the real value-added growth of the digital economy accounted for 25% of total real GDP growth.[5]

Figure 1. Effect on World GDP (percent)



Source: Gary Clyde Hufbauer and Zhiyao Lu, "Can Digital Flows Compensate for Lethargic Trade and Investment?," Peterson Institute for International Economics, November 28, 2018.

Notes: Global internet traffic, measured in petabyte per month. Merchandise trade and FDI are normalized by dividing flows by world GDP; data flow is normalized by dividing flows by world population.

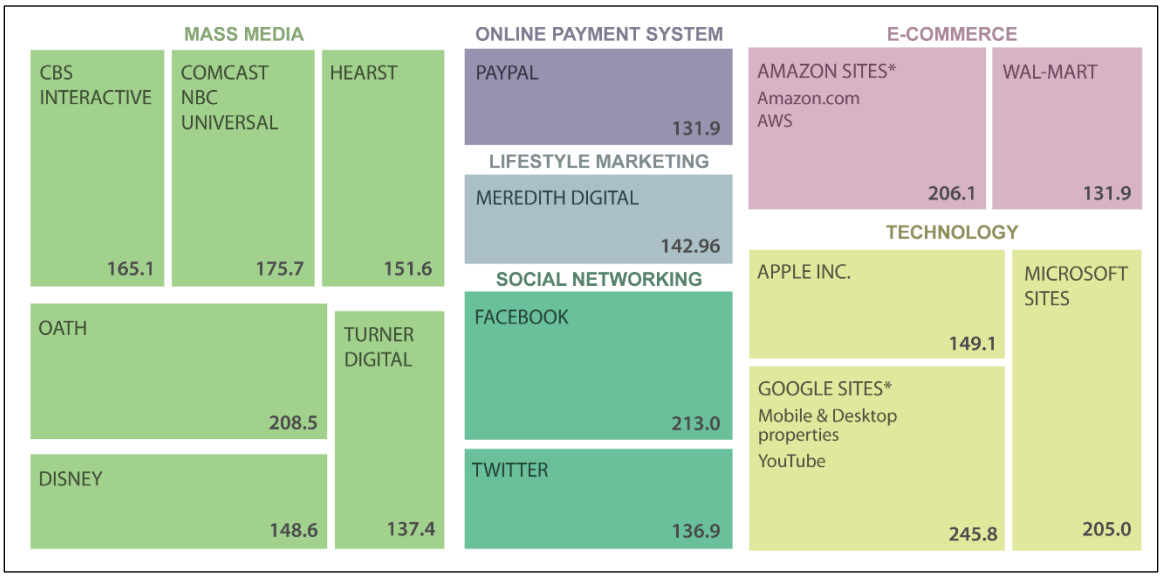
[4] Gary Clyde Hufbauer and Zhiyao (Lucy) Lu, "Can Digital Flows Compensate for Lethargic Trade and Investment?" Peterson Institute of International Economics, November 28, 2018.

[5] U.S. Bureau of Economic Analysis, *Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accounts*, March 2018, p.6.

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 use the internet, including 95% of people in North America.[6] As of 2017, 75% of U.S. households use wired internet access, but an increasing number rely on mobile internet access as the internet is integrated into people's everyday lives; 72% of U.S. adults own a smartphone.[7] As of the end of 2018, approximately 40% of internet traffic in the United States came from mobile devices.[8] Each day, companies and individuals across the United States depend on the internet to communicate and transmit data via various media and channels that continue to expand with new innovations (see **Figure 2**).

Figure 2. Snapshot of Most Popular Websites

December 2018, Millions of unique U.S. visitors



Source: Statistica.com.

Note: * Examples of web properties owned by multinational companies.

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 are the drivers of globalization and interconnectedness. The highest levels reportedly are those flows between the United States and Western Europe, Latin America, and China. 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.[9] ICT spending is a large and growing component of the international economy and essential to digital trade and innovation.

[6] Internet World Stats, *World Internet Usage and Population Statistics*, June 30, 2018, https://internetworldstats.com/stats.htm.

[7] U.S. International Trade Commission, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, Publication Number: 4716, Investigation Number: 332-561, August 2017, p.47-49, https://www.usitc.gov/publications/332/pub4716.pdf.

[8] Statistica, "Percentage of mobile device website traffic in the United States from 1st quarter 2015 to 4th quarter 2018," 2019, https://www.statista.com/statistics/683082/share-of-website-traffic-coming-from-mobile-devices-usa/.

[9] 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.

According to the United Nations, world trade in ICT physical goods grew to $2 trillion in 2017 with U.S. ICT goods exports over $146 billion.[10]

Semiconductors, a key component in many electronic devices, are a top U.S. ICT export. Global sales of semiconductors were $468.8 billion in 2018, an increase of 6.81% over the prior year.[11] U.S.-based firms have the largest global market share with 45% and accounted for 47.5% of the Chinese market. Given the importance of semiconductors to the digital economy and continued advances in innovation, countries such as China are seeking to grow their own semiconductor industry to lessen their dependence on U.S. exports.

ICT services are outpacing the growth of international trade in ICT goods. The OECD estimates that ICT services trade increased 40% from 2010 to 2016. The United States is the fourth-largest OECD exporter of ICT services, after Ireland, India, and the Netherlands.[12] 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. In 2017, exports of ICT services grew to $71 billion of U.S. exports while services exports that could be ICT-enabled were another $439 billion, demonstrating the impact of the internet and digital revolution.[13]

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.[14] According to one estimate, software contributed more than $1.14 trillion to the U.S. value added to GDP in 2016, an increase of 6.4% over 2014, and the U.S. software industry accounted for 2.9 million jobs directly in 2016.[15] Internet-advertising, an industry that would not exist without ICT, generated an additional 10.4 million U.S. jobs.[16]

[10] https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=15850.

[11] Semiconductor Industry Association, 2019 SIA Factbook, 2019.

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

[13] 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.

[14] U.S. Bureau of Economic Analysis, *Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accoun*ts, March 2018, p.9.

[15] EIU estimates, "The Growing $1 Trillion Economic Impact of Software," software.org.

[16] John Deighton, "Economic Value of the Advertising-Supported Internet Ecosystem," 2017, https://www.iab.com/wpcontent/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf.

Figure 3. What is Digital Trade?

Examples of international digital trade

Source: CRS.

Note: The above graphic is illustrative only and is not based on a real business or reflective of all aspects of digital trade.

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 (see **Figure 3**). 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 add value by raising productivity and/or lowering the costs and barriers related to flows of traditional goods and services. For example, companies may rely on radio-frequency identification (RFID)

tags for supply chain tracking, 3-D printing based on data files, or devices or objects connected via the Internet of Things (see **text box**). In addition, digital platforms serve as intermediaries for multiple forms of digital trade, including e-commerce, social media, and cloud computing. In these ways, digitization pervades every industry sector, creating challenges and opportunities for established and new players.

Looking at digital trade in an international context, approximately 12% of physical goods are traded via international e-commerce.[17] Global e-commerce grew from $19.3 trillion in 2012 to $27.7 trillion in 2016, of which 86% was business-to-business (B2B).[18] One source estimates that cross-border business-to-consumer (B2C) e-commerce sales will reach approximately $1 trillion by 2020.[19]

These estimates do not quantify the additional benefits of digitization upon business efficiency and productivity, or of increased customer and market access, which enable greater volumes of international trade for firms in all sectors of the economy. Digitization efficiencies have the potential to both increase and decrease international trade. 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; at the same time, however, automation, Artificial Intelligence (AI), and 3-D printing could enable more local production, thereby reducing global trade by as much as 10% by 2030.[20] The overall impact of digitization has yet to be seen.

One study coined the term "digital spillovers" to fully capture the digital economy and estimated the global digital economy, including such spillovers, was $11.5 trillion in 2016, or 15.5% of global GDP.[21] Their analysis indicated that the long-term return on investment (ROI) for digital technologies is 6.7 times that of nondigital investments.[22]

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.[23] For example, 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.[24] The initiative aims to expand to include several multinational food suppliers, farmers, and retailers and depends on connections via the Internet of Things and open international data flows. With increased applications, the Internet of Things may have a global economic impact of as much as $11.1 trillion per year, according to one study.[25]

---

[17] Jacques Bughin and Susan Lund, "The ascendancy of international data flows," *VOX*, January 9, 2017.

[18] U.S. International Trade Commission, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, Publication Number: 4716, Investigation Number: 332-561, August 2017, p.13, https://www.usitc.gov/publications/332/pub4716.pdf.

[19] Susan Lund et al., "Globalization in transition: The future of trade and value chains," *McKinsey*, January 2019.

[20] Ibid.

[21] Huawei Technologies and Oxford Economics, *Digital Spillover*, http://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf.

[22] Ibid.

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

[24] Roger Aitken, "IBM & Walmart Launching Blockchain Food Safety Alliance In China With Fortune 500's JD.com," *Forbes*, December 14, 2017.

[25] Alexandre Menard, "How can we recognize the real power of the Internet of Things?" *McKinsey*, November 2017.

Key Emerging Technologies

Internet of Things (IoT)

"encompass(es) all devices and objects whose state can be read or altered via the internet, with or without the active involvement of individuals.... The internet of things consists of a series of components of equal importance—machine-to-machine communication, cloud computing, big data analysis, and sensors and actuators. Their combination, however, engenders machine learning, remote control, and eventually autonomous machines and systems, which will learn to adapt and optimise themselves."[26]

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)."[27]

Artificial Intelligence (AI)

"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."[28]

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 disrupted.[29] 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.[30]

The internet, and cloud services specifically, has been called the great equalizer, since it allows small companies access to the same information and the same computing power as large firms using a flexible, scalable, and on-demand model. For example, Thomas Publishing Co., a U.S. mid-sized, private, family-owned and -operated business, is transporting data from its own computer servers to data centers run by Amazon.com Inc.[31] Digital platforms can minimize costs and enable small and medium-sized enterprises (SMEs) to grow through extended reach to customers or suppliers or integrating into a global value chain (GVC). More than 50% of businesses globally rely on data flows for cloud computing (see **text box**).[32]

Digitization of customs and border control mechanisms also helps 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.[33] With simpler border and customs processes, more firms are able to

[26] OECD (2015), *OECD Digital Economy Outlook 2015*, p. 61, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264232440-2-en

[27] For more information, see CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

[28] For more information, see CRS In Focus IF10608, *Overview of Artificial Intelligence*, by Laurie A. Harris.

[29] 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.

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

[31] Jay Greene, "Amazon to Launch Cloud Migration Service," *The Wall Street Journal*, March 15, 2016.

[32] U.S. International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, Investigation Number: 332-561, August 2017.

[33] Commercial Customs Operations Advisory Committee (COAC), *Trade Progress Report*, November 2017,

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 97% export, while that number is a full 100% in countries as diverse as Peru and Ukraine.[34] Netflix, a U.S. firm offering online streaming services, increased its international revenue from $4 million in 2010 to more than $5 billion in 2017.[35]

A Local Manufacturer Grows Through Digital Trade

Kirk Anton and Tricia Hudson launched their business in 2010 as a one-stop shop for heat transfer materials, importing heat-applied materials and creating customized products for clients. The company moved online and converted to completely digital in 2013, using services such as Google Analytics to inform their marketing campaigns. Growing by more than 70% over four years, in 2017 the company employed forty people in Florida, Kentucky, Nevada, and North Dakota, and boasted over 85,000 customers across the globe.[36]

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. According to one official of the Asia-Pacific Economic Cooperation Forum (APEC), technology has enabled SMEs to open in new sectors such as ride-sharing and online order delivery services, and provides them with a "bigger, better opportunity to grow and learn that to join a global value chain."[37] Another 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.[38] However, the costs of digital trade can be concentrated on particular sectors (see next section).

Digitization Challenges

The U.S. digital economy supported 3.3% of total U.S. employment in 2017, and those jobs earned approximately one and a half times the average annual worker compensation of the overall U.S. economy, making them attractive source for future growth.[39] Software, and the software industry, contributes to the GDP in all 50 states, with the value-added GDP of the software industry growing more than 40% in Idaho and North Carolina.[40] Industries, such as media and firms in urban centers, account for a larger share of the benefits. 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.

---

https://www.cbp.gov/sites/default/files/assets/documents/2017-Nov/Global%20Supply%20Chain%20Subcommittee%20Trade%20Executive%20Summary%20Nov%202017.pdf.

[34] James Manyika, Sree Ramaswamy, and Somesh Khanna et al., *Digital America: A Tale of the Haves and Have-Mores*, McKinsey Global Institute, December 2015, p. 40, http://www.mckinsey.com/industries/high-tech/our-insights/digital-america-a-tale-of-the-haves-and-have-mores.

[35] World Trade Organization, "World Trade Report 2018: The future of world trade," p.10, 2018, https://www.wto.org/english/res_e/publications_e/wtr18_e.htm.

[36] Google, *Economic Impact United States 2017*, https://economicimpact.google.com/.

[37] APEC, "APEC's Startup Revolution Brings the Next Big Thing," November 2, 2017; https://www.apec.org/Press/Features/2017/1102_interview.

[38] 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.

[39] U.S. Bureau of Economic Analysis, *Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry Economic Accoun*ts, March 2018, p.2.

[40] Software.org, "The Growing $1 Trillion Economic Impact of Software," https://software.org/reports/2017-us-software-impact/.

However, sources of "e-friction" or obstacles can prevent consumers, companies, and countries from realizing the full benefits of the online economy.[41] Causes of e-friction can fall into four categories: infrastructure, industry, individual, and information. Government policy can influence e-friction, from investment in infrastructure and education to regulation and online content filtering. According to some experts, economies with lower amounts of e-friction may be associated with larger digital economies.[42]

While there are numerous positive digital dividends, there are also possible negative and uneven results across populations, such as the displacement of unskilled workers, an imbalance between companies with and without internet access, and the potential for some to use the internet to establish monopolies.[43] 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. For example, one study found a mismatch between workforce skills and job openings such as in Nashville, TN, which has an abundance of workers with music production and radio broadcasting skills but a scarcity of workers with IT infrastructure, systems management, and web programming skills.[44] Another source notes over 11,000 open computing jobs in Michigan, with average salaries of over $80,000.[45]

The World Bank identified policy areas to try to ensure, and maintain, the potential benefits of digitization. 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. According to the World Economic Forum Global Competitiveness Index 4.0, the United States is ranked at the top with a score of 85.6% compared to the global median score of 60%.[46] The study identifies the key drivers of productivity as human capital, innovation, resilience, and agility, noting that future productivity depends not only on investment in technology but investment in digital skills. While the United States is considered a "super innovator," the report also notes "indications of a weakening social fabric … and worsening security situation … as well as relatively low checks and balances, judicial independence, and transparency."[47]

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.[48] Over two-thirds of U.S. jobs created since 2010 require some level of digital skills.[49] The OECD found that generic ICT skills are insufficient among a significant percentage

---

[41] Paul Zwillenberg, Dominic Field, and David Dean, *Greasing the Wheels of the Internet Economy*, Boston Consulting Group, February 2014, https://www.bcgperspectives.com/content/articles/digital_economy_telecommunications_greasing_wheels_internet_economy/.

[42] Ibid.

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

[44] Penny Pritzker and John Engler, Director Edward Alden, *The Work Ahead: Machines, Skills, and U.S. Leadership in the Twenty-First Century, Independent Task Force Report*, Council of Foreign Relations, April 2018.

[45] https://code.org/promote/mi.

[46] World Economic Forum, Global Competitiveness Report 2018, p. 10, http://www3.weforum.org/docs/GCR2018/05FullReport/TheGlobalCompetitivenessReport2018.pdf.

[47] Ibid, p. 33.

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

[49] Penny Pritzker and John Engler, Director Edward Alden, *The Work Ahead: Machines, Skills, and U.S. Leadership in*

of the global workforce and few countries have adopted comprehensive ICT skills strategies to help workers adapt to changing jobs.[50]

Digital Trade Policy and Barriers

Policies that affect digitization in any one country's economy can have consequences beyond its borders, and because the internet is a global "network of networks," the state of a country's digital economy can have global ramifications. Protectionist policies may erect barriers 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 gains. What some policymakers see as protectionist, however, others may view as necessary to protect domestic interests. For examples of the types of digital trade barriers that are in place around the globe, please see Appendix.

Despite common core principles such as protecting citizen's privacy and expanding economic growth, governments face multiple challenges in designing policies around digital trade. The 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.[51]

Ensuring a free and open internet is a stated policy priority for the U.S. government.[52] Like other cross-cutting policy areas, such as cybersecurity or privacy, no one federal entity has policy primacy on all aspects 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.[53]

the Twenty-First Century, Independent Task Force Report, Council of Foreign Relations, April 2018.

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

[51] 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.

[52] http://www.state.gov/e/eb/cip/netfreedom/index.htm.

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

Protect a Free and Open Internet[54]

Protecting a free and open internet is a policy priority as stated in President Trump's 2017 *National Security Strategy*.

"The United States will advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services. The United States will promote the free flow of data and protect its interests through active engagement in key organizations, such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), the UN, and the International Telecommunication Union (ITU)."

The Department of Commerce works to promote U.S. digital trade policies domestically and abroad. In 2015, Commerce launched a Digital Economy Agenda that identifies four pillars:[55]

1. "Promoting a free and open Internet worldwide, because the Internet functions best for our businesses and workers when data and services can flow unimpeded across borders";
2. "Promoting trust online, because security and privacy are essential if electronic commerce is to flourish";
3. "Ensuring access for workers, families, and companies, because fast broadband networks are essential to economic success in the 21st century"; and
4. "Promoting innovation, through smart intellectual property rules and by advancing the next generation of exciting new technologies."

Commerce's digital attaché program under the foreign commercial service helps U.S. businesses navigate regulatory issues and overcome trade barriers to e-commerce exports in key markets.[56]

The Administration also works to promote U.S. digital priorities by identifying and challenging foreign trade barriers and through trade negotiations. As with traditional trade barriers, digital trade constraints can be classified as tariff or nontariff barriers. Tariff barriers may be imposed on 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. Often, such barriers are intended to protect domestic producers and suppliers. Some estimates indicate that removing foreign barriers to digital trade could increase annual U.S. real GDP by 0.1%-0.3% ($16.7 billion-$41.4 billion), increase U.S. wages up to 1.4%, and add up to 400,000 U.S. jobs in certain digitally intensive industries.[57]

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

[55] Alan B Davidson, "The Commerce Department's Digital Economy Agenda," November 9, 2015, https://www.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.

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

[57] Digitally intensive industries include sectors in communications, finance, trade, other services, and manufacturing.

U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, Publication No: 4485, Investigation No: 332-540, August 2014, pp. 106-108, https://www.usitc.gov/publications/332/pub4485.pdf.

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.[58] TPA 2015 objectives related to digital trade direct 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.

Tariff Barriers

Historically, trade policymakers focused on overt trade barriers such as tariffs on products entering countries from abroad. 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.

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

U.S. ICT services are often inputs to final demand products that may be exported by other countries, such as China. U.S. ICT services have shown increasing growth rates since the middle of 2014.[59]

[58] For more information on TPA, 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.

[59] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, p. 120, http://dx.doi.org/10.1787/9789264276284-en.

ICT Goods Tariff Barriers: Selected Examples

Brazil, Mexico, and Vietnam are key participants in the ICT goods market and impose high tariffs on non-FTA partners. According to the United Nations Statistics Division, in 2015 Brazil reported $1.3 billion in medical ICT equipment imports, such as electrocardiographs, ultrasound devices, and magnetic resonance imaging devices,[60] despite tariffs of up to 16% on these products.[61]

In 2014, Vietnam reportedly imported $10.3 billion worth of electronic integrated circuits (microchips) and parts, including approximately 4% or $398 million from the United States.[62] While Vietnam imposes no tariffs on these product categories, several ICT items in Vietnam's tariff schedule have high applied rates, including multiple categories of radio equipment, which have an applied rate as high as 30% according to the WTO.[63]

Nontariff Barriers

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

Nondiscrimination between local and foreign suppliers is a core principle encompassed in global trading rules and U.S. free trade agreements. 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.

Potential Barriers to Digital Trade

- High tariffs
- Localization requirements
- Cross border data flow limitations
- IPR infringement
- Discriminatory, unique standards or burdensome testing
- Filtering or blocking
- Restrictions on electronic payment systems or the use of encryption
- Cybertheft of U.S. trade secrets
- Forced technology transfer

Broader governance issues, including rule of law, transparency, and investor protections, can pose barriers and limit the ability of firms and individuals to successfully 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 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.[64] Governments often use privacy protection or national security arguments as justifications for these measures. Though localization policies can be used to achieve legitimate public policy objectives, some are designed to protect, favor, or

[60] Data on Harmonized System code 9018 from U.N. Comtrade: http://comtrade.un.org.

[61] CRS analysis of tariff data from the WTO Tariff Analysis Online (TAO): https://tao.wto.org.

[62] U.S. Census Bureau.

[63] Harmonized System code 8527, from WTO TAO.

[64] 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.

stimulate domestic industries, service providers, or intellectual property at the expense of foreign counterparts and, in doing so, function as nontariff barriers to market access. In recent free trade agreements, 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, data localization was the most cited policy measure impeding digital trade, and the number of data localization measures globally has doubled in the last six years.[65] One study found that over 120 countries have laws related to personal data protection, often requiring data localization.[66] 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. 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.[67]

Data localization requirements pose barriers to companies' efforts to operate more efficiently by migrating to the cloud or to SMEs attempting to enter new markets. According to some estimates, cloud computing accounted for 70% of related IT market growth between 2012 and 2015, and is expected to represent 60% of growth through 2020.[68] Most of the largest global providers of cloud computing services are U.S. companies (Amazon, Microsoft, Google, and IBM).

Regulations or policies that limit data flows create barriers to firms and countries seeking to consume cloud services. One U.S. business group noted increased forced localization measures, citing examples in China, Colombia, the European Union (EU), Indonesia, South Korea, Russia, and Vietnam.[69] The Business Software Alliance's 2018 Global Cloud Computing Scorecard highlighted barriers to cloud services in Indonesia, Russia, and Vietnam.[70] For example, to comply with localization requirements and continue to serve consumers of Google's many cloud services (e.g., Gmail, search, maps) globally, the company is opening more data centers in the United States and internationally.[71]

---

[65] https://www.usitc.gov/publications/332/pub4716.pdf

[66] C&M International, "Benefits of the APEC Cross-Border Privacy Rules," October 2018, https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf.

[67] 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.

[68] Mark Brinda and Michael Heric, "The Changing Faces of the Cloud: Technology Companies Are Adapting to Sell Cloud to the Growing Number of More-Mainstream Buyers," Bain & Company, 2017.

[69] Information Technology Industry Council, Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses, August 1, 2017, http://www.itic.org/dotAsset/9d22f0e2-90cb-467d-81c8-ecc87e8dbd2b.pdf.

[70] Business Software Alliance, *2018 BSA Global Cloud Computing Scorecard*, http://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf.

[71] Google Cloud Platform Blog, "Google Cloud Platform adds two new regions, 10 more to come," March 22, 2016,

Finding a global consensus on how to balance open data flows, cybersecurity, and privacy protection may be key to maintaining trust in the digital environment and advancing international trade.[72] 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").

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).

In April 2018, the Commerce Department announced plans to develop a "comprehensive strategy to address trade-related forced localization policies, practices, and measures impacting the U.S. information and communications technology (ICT) hardware manufacturing industry."[73] In creating a strategic response to the increase in protectionist localization policies globally, Commerce aims to preserve the competitiveness of the U.S. ICT sector.[74]

Examples of Localization Barriers

Examples of localization barriers include the following:

- In **China**, measures across multiple sectors (e.g., banking) require "secure and controllable" technology, mandating suppliers purchase Chinese products and use Chinese suppliers (see "China").
- In **Turkey**, the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions requires firms to maintain documents, records, data storage, and processing facilities in Turkey.
- In **Nigeria**, the government requires ICT companies to use Nigerian companies for the provision of at least 80% of all value-added services on their network, without clearly defining "value-added services."
- In **India**, the 2015 National Telecom M2M ("machine to machine") roadmap recommends preferences for locally manufactured SIM cards and domestically sourced goods.

Source: *2019 National Trade Estimate Report on Foreign Trade Barriers*, Office of the United States Trade Representative, March 2019.

Intellectual Property Rights (IPR) Infringement

While the internet and digital technologies have opened up markets for international trade, they also present ongoing and unique challenges for the protection and enforcement of intellectual property (IP), which are creations of the mind—such as an invention, literary/artistic work, design, symbol, name, or image—embodied in a physical or digital object. Intellectual property rights (IPR)[75] are legal, private, enforceable, time-limited rights that governments grant to

https://cloudplatform.googleblog.com/2016/03/announcing-two-new-Cloud-Platform-Regions-and-10-more-to-come_22.html?mod=djemCIO_h.

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

[73] Department of Commerce, "U.S. Strategy To Address Trade-Related Forced Localization Barriers Impacting the U.S. ICT Hardware Manufacturing Industry," 83 *Federal Register* 15786, April 12, 2018.

[74] The planned strategy will not address cross-border data flow restrictions.

[75] See CRS Report RL34292, *Intellectual Property Rights and International Trade*, by Shayerah Ilias Akhtar and Ian F. Fergusson; and CRS In Focus IF10033, *Intellectual Property Rights (IPR) and International Trade*, by Shayerah Ilias

inventors and artists to exclude others from using their creations without their permission. Examples of IPR include patents, copyrights, trademarks, and trade secrets.

Innovations in digital technologies fuel IPR infringement by enabling 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. The internet provides "ease of conducting commerce through unverified vendors, inability for consumers to inspect goods prior to purchase, and deceptive marketing."[76] Both copyright- and trademark-based industries face challenges tackling not only infringement in physical marketplaces, but increasingly also online marketplaces.[77] Cyber-enabled theft of trade secrets is of growing concern. Trade secrets are essential to many businesses' operations and important assets, including those in ICT, services, biopharmaceuticals, manufacturing, and environmental and other technologies.

IPR infringement in the digital environment is particularly difficult to quantify but considered to be significant, potentially exceeding the volume of sales through traditional physical markets.[78] A 2016 industry study estimated the value of digitally pirated music, movies, and software (not actual losses) to be $213 billion in 2013 and growing to as much as $384-$856 billion in 2022.[79] The IP Commission estimated that the annual cost to the U.S. economy from counterfeit goods, pirated software, and theft of trade secrets continues to surpass $225 billion and could reach $600 billion.[80]

Efforts to address IPR infringement raise issues of balance about, on one hand, protecting and enforcing IPR to protect the rights of content holders and incentivize innovation in the digital environment and, on the other hand, setting appropriate limitations and exceptions to ensure other economically and socially valuable uses. Content industries say that IP theft costs them sales, detracts from legitimate services, harms investors in these businesses, damages their brand or reputation, and hurts "law-abiding" consumers. Some technology product and service companies, as well as some civil society groups, assert that overly stringent IPR policies may stifle information flows and legitimate digital trade and these groups support "fair use" exceptions and limitations to IPR.[81]

Akhtar and Ian F. Fergusson.

[76] USTR, *2015 Out-of-Cycle Review of Notorious Markets*, December 2015, p. 9.

[77] USTR, 2017 Out-of-Cycle Review of Notorious Markets, January 2018.

[78] USTR, *2017 Special 301 Report*, April 2017.

[79] Frontier Economics, *The Economic Impacts of Counterfeiting and Piracy*, report commissioned by Business Action to Stop Counterfeiting and Piracy (BASCAP) of the International Chamber of Commerce (ICC) and the International Trademark Association (INTA), June 2017.

[80] The estimate does not include patent infringement. Commission on the Theft of American Intellectual Property ("IP Commission"), *The Theft of American Intellectual Property: Reassessments of the Challenge and U.S. Policy—Update to the IP Commission Report, 2017*. The IP Commission describes itself as an "independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academia, and politics."

[81] "Fair use" is a doctrine recognized in U.S. law that permits limited use of copyrighted works without requiring permission from the rights holder in certain cases, such as criticism, comment, news reporting, research, scholarship, and teaching.

New EU Copyright Rules

The EU's new copyright directive highlights the debate over balance, and has implications for U.S. digital trade. On April 15, 2019, the EU adopted the new rules to modernize its copyright laws to adapt to the digital environment. One objective of the directive is to create a fairer marketplace for online content for creators and press. 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 will have to negotiate licenses from newspapers and other publishers for showing content that is under two-years-old on their news feeds. Short extracts from press publications—sometimes called "snippets"—are outside of the scope of the rule.[82] 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. If no licensing agreement exists between creators and the online platforms, YouTube and other such 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. Some U.S. stakeholders, such as the publishing industry, support the new rules, while others, including U.S. businesses that are content-aggregators, have raised concerns about increased costs, market access barriers, and effects on the innovation environment of the new rules.[83] After the publication of the directive in the Official Journal of the EU, member states will have 24 months to transpose the new rules into their national law.

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 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 IPR 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 USITC 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 make it difficult for firms to enter a particular market. 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, and is an often-cited concern for U.S. businesses facing delays getting products to market.[84] 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).

[82] European Commission, "Question & Answers: EU Negotiators Reach a Breakthrough to Modernise Copyright Rules," press release, February 13, 2019.

[83] USTR, *2019 National Trade Estimate Report on Foreign Trade Barriers*, March 2019.

[84] USTR, *2019 National Trade Estimate Report on Foreign Trade Barriers*, March 2019, p. 242.

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. Governments that filter or block websites, or otherwise impede access, form another type of nontariff barrier. For example, China has asserted a desire for "digital sovereignty" and has erected what is termed by some as the "Great Firewall." A change to China's internet filters also blocks virtual private network (or VPN) access to sites beyond the Great Firewall. VPNs have been used by Chinese citizens to use websites like Facebook and by companies to access data outside of China (e.g., information from foreign subsidiaries or partners).[85]

While China is the most well-known, it is not alone in seeking to control access to websites. For example, Thailand established a Computer Data Filtering Committee to use the court system to block websites that it views as violating public order and good order, as well as intellectual property.[86] In Russia, citizens protested government censorship, including the blocking of a popular messaging application along with other websites and online tools.[87]

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.[88] 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.[89] 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.[90] 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

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

[86] USTR, *2018 National Trade Estimate Report on Foreign Trade Barriers*, March 2018, p. 446.

[87] Neil MacFarquhar, "'They Want to Block Our Future': Thousands Protest Russia's Internet Censorship," *The New York Times*, April 30, 2018.

[88] Adam Satariano, "Britain Proposes Broad New Powers to Regulate Internet Content," *The New York Times*, April 7, 2019.

[89] 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.

[90] For more information on net neutrality, see CRS Report R40616, *The Net Neutrality Debate: Access to Broadband Networks*, by Angele A. Gilroy.

other unlawful actions. Cybersecurity can also be an important tool in protecting privacy and preventing unauthorized surveillance or intelligence gathering.[91] 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. According to the White House Council of Economic Advisers, malicious cyberactivity (i.e., business disruption, theft of proprietary information) cost the U.S. economy up to $109 billion in 2016.[92] Cybersecurity risks run across all industry sectors that rely on digital information. In the entertainment industry, for example, Iranian hackers stole unreleased episodes of HBO's "Game of Thrones" series, holding them for ransom, and potentially costing the company and risking intellectual property and harm to the corporate reputation.[93] The Federal Bureau of Investigations (FBI) suspects Chinese hackers were behind a cyberattack on the Marriot's Starwood hotel chain that resulted in potentially stealing IPR and the personal information of up to 327 million hotel customers, including their birthdates and passport numbers.[94] An FBI official testified to the Senate Judiciary Committee that Chinese espionage efforts have become "the most severe counterintelligence threat facing our country today."[95]

Cybersecurity threats can disrupt business operations or supply chains. The 2017 WannaCry ransomware attack impacted public and private sector entities in over 150 countries with direct costs of at least $8 billion due to computer downtime, according to one estimate.[96] In the widespread attack, computers in homes, schools, hospitals, government agencies, and companies were hit. The United States publicly attributed the cyberattack to North Korea, stating that "these disruptions put lives at risk."[97] Compromises of ITC supply chains can also pose a threat to organizations that rely on the tampered hardware as was alleged, for example, with some Supermicro microchips used in ITC manufacturing in China.[98]

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.[99] However, restrictions on the ability for a firm to use encryption may make a

---

[91] For more information on cybersecurity, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer, and CRS In Focus IF10559, *Cybersecurity: An Introduction*, by Chris Jaikaran.

[92] 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.

[93] Nicole Hong, "Iranian Charged With Hacking HBO, Taking 'Game of Thrones' Scripts," *Wall Street Journal*, November 21, 2017.

[94] David E. Sanger et al, "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *The New York Times*, December 11, 2018.

[95] U.S. Congress, Senate Committee on the Judiciary, *China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses*, 115th Cong., December 12, 2018.

[96] Nick Kostov, Jeannette Neumeann, and Stu Woo, "Cyberattack Victims Begin to Assess Financial Damage," *Wall Street Journal*, May 14, 2017.

[97] Thomas P. Bossert, Assistant to the President for Homeland Security and Counterterrorism, "It's Official: North Korea Is Behind WannaCry," *Wall Street Journal*, December 18, 2017.

[98] Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," Bloomberg, October 4, 2018.

[99] 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*

company vulnerable to cyberattacks or cybertheft, demonstrating the need for policies and regulations to balance competing objectives.

U.S. Digital Trade with Key Trading Partners

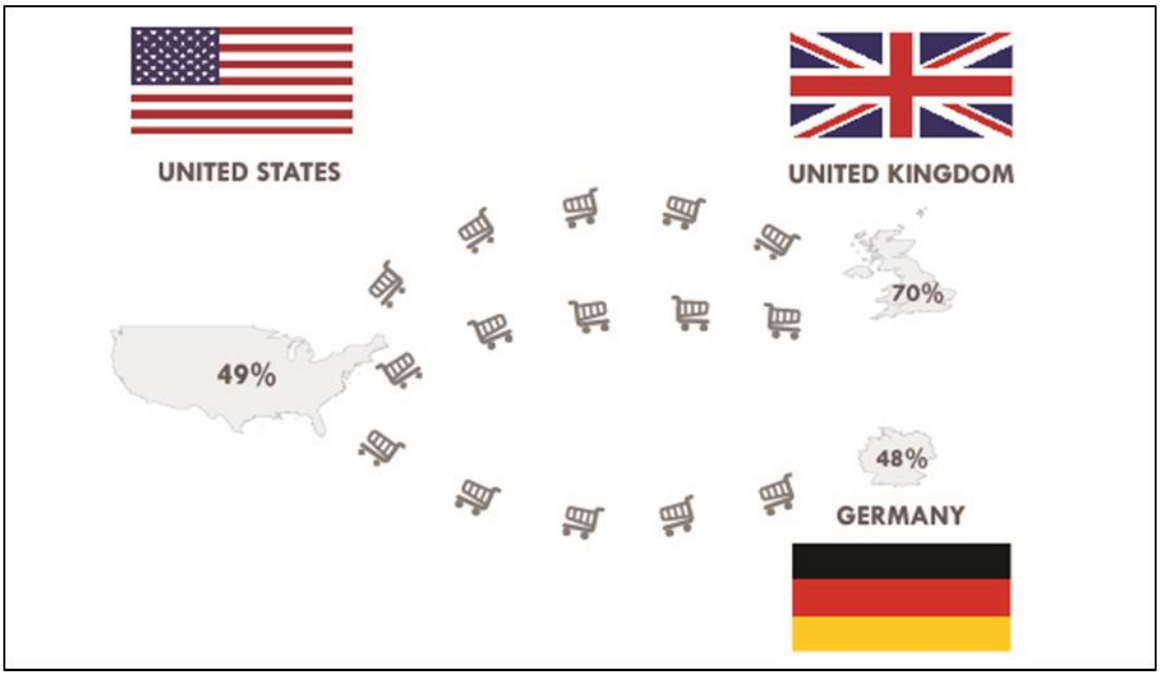
The European Union (EU) and China are large U.S. digital trade partners and each has presented various challenges for U.S. companies, consumers, and policymakers.

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 transatlantic economy is the largest in the world, and cross-border data flows between the United States and EU are the highest in the world. In between 2003 and 2017, total U.S.-EU trade in goods and services (exports plus imports) nearly doubled from $594 billion to $1.2 trillion.[100] ICT and potentially ICT-enabled services accounted for approximately $190 billion of U.S. exports to the EU in 2017.[101] The two sides also account for a significant portion of each other's e-commerce trade (see **Figure 4**).

Figure 4. Select U.S.-EU Cross-Border E-Commerce Purchases



Source: Kati Souminen, "Where the Money Is: The Transatlantic Digital Market," CSIS, October 12, 2017.

Issues, by Richard M. Thompson II and Chris Jaikaran.

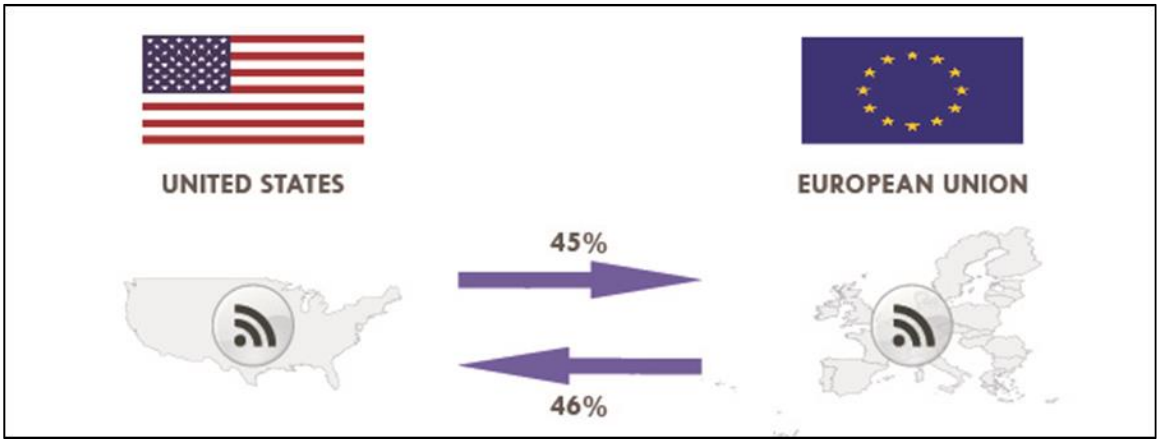
[100] See CRS In Focus IF10930, *U.S.-EU Trade and Investment Ties: Magnitude and Scope*, by Shayerah Ilias Akhtar.

[101] https://apps.bea.gov/iTable/iTable.cfm?ReqID=62&step=1.

Notes: 48% of German and 70% of UK shoppers purchase from U.S. e-commerce sites. 49% of U.S. e-commerce purchases are from UK sites.

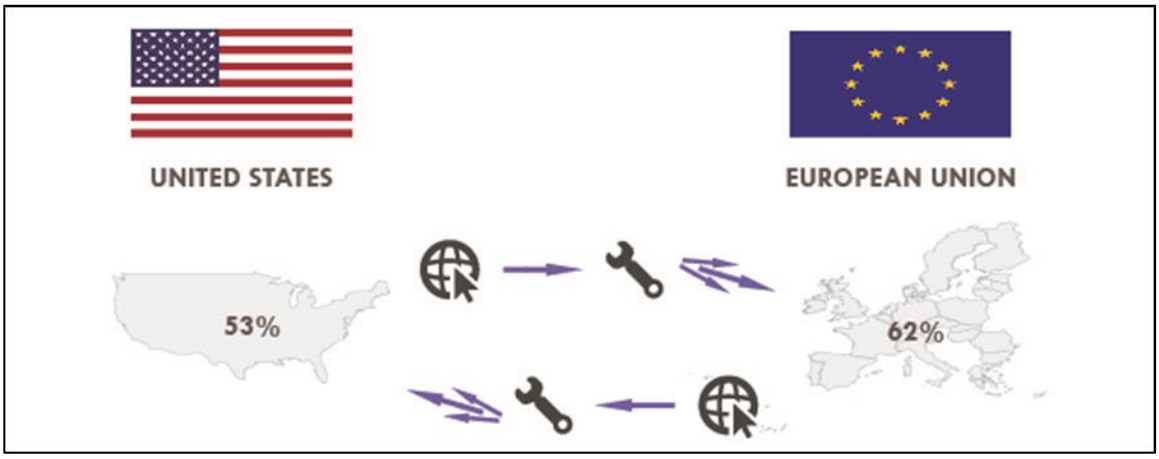
The United States and EU account for almost half of each other's digitally deliverable service exports (e.g., business, professional, and technical services) and many of these services are incorporated into exported goods as part of GVCs (see **Figure 5** and **Figure 6**).[102] The UK alone accounted for 23% of U.S. digitally deliverable services exports.[103] Almost 40% of the data flows between the United States and EU are through business and research networks.[104]

Figure 5. Digitally Deliverable Service Exports 2017



Source: "Where the Money Is: The Transatlantic Digital Market," CSIS, October 12, 2017.

Figure 6. Digitally Deliverable Services Incorporated into Global Value Chains



Source: "Where the Money Is: The Transatlantic Digital Market," CSIS, October 12, 2017.

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. To address some of these differences, in 2013, the United States and the EU began, but did not

[102] Where the Money Is: The Transatlantic Digital Market," CSIS, October 12, 2017.

[103] Ibid.

[104] All figures on U.S.-EU trade and data flows includes the United Kingdom (UK) as part of the EU. Without the UK, the statistics would be lower.

conclude, negotiating a broad FTA. Negotiations included a number of digital trade issues such as market access for digital products, IPR protection and enforcement, cybersecurity, and regulatory cooperation, among other things.[105] On October 16, 2018, the Trump Administration notified Congress under Trade Promotion Authority (TPA) of its intent to enter into negotiations with the EU. The Administration's specific negotiating objectives envision a wide-ranging agreement, including addressing digital trade, along with trade in goods, services, agriculture, government procurement, and other rules, such as on IPR and investment.[106] However, no agreement exists on the scope of the negotiations. The EU negotiating mandates, in contrast, are narrower; they authorize EU negotiations with the United States to address industrial tariffs (excluding agricultural products) and nontariff regulatory barriers to make it easier for companies to prove that their products meet U.S. and EU technical requirements.[107]

The Administration also notified Congress under TPA of its intent to negotiate a trade agreement with the UK post-Brexit, and the corresponding specific negotiating objectives likewise envision a broad agreement addressing digital trade issues. The UK cannot formally negotiate or conclude a new agreement until it exits the EU, which has exclusive competence over trade policy and negotiates trade deals on behalf of all EU member states. Details about the future UK-EU trade relationship remain largely unknown, and it is uncertain when and to what extent the UK will regain control of its national trade policy—a major objective for Brexit supporters. These factors directly shape prospects for a proposed bilateral U.S.-UK free trade agreement.[108]

EU-U.S. Privacy Shield

The United States and EU have different legal approaches to information privacy that extends into the digital world. After extensive negotiations, the EU-U.S. Privacy Shield entered into force on July 12, 2016, creating a framework to provide U.S. and EU companies a mechanism to comply with data protection requirements when transferring personal data between the EU and the United States.[109] Under the Privacy Shield program, U.S. companies can voluntarily self-certify compliance with requirements such as robust data processing obligations. The agreement includes obligations on the U.S. government to proactively monitor and enforce compliance by U.S. firms, establish an ombudsman in the U.S. State Department, and set specific safeguards and limitations on surveillance. The United States and Switzerland also agreed to the Swiss-U.S. Privacy Shield, which will be "comparable" to the EU-U.S. agreement.[110]

The Privacy Shield also involves an annual joint review by the United States and the EU, the second of which was completed in October 2018.[111] Under the review, the commission found that

[105] 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.

[106] Office of the U.S. Trade Representative, United States-European Union Negotiations: Summary of Specific Negotiating Objectives, January 2019. For more information, see CRS In Focus IF10931, *U.S.-EU Trade and Economic Issues*, by Shayerah Ilias Akhtar.

[107] Council of the EU, "Trade with the United States: Council authorises negotiations on elimination of tariffs for industrial goods and on conformity assessment," press release, April 15, 2019.

[108] CRS In Focus IF11123, *Brexit and Outlook for U.S.-UK Trade Agreement*, by Shayerah Ilias Akhtar.

[109] For more information on the Privacy Shield, see https://www.privacyshield.gov/Program-Overview.

[110] Lauren Cerulus, "Switzerland and U.S. strike 'privacy shield' data transfer deal," *Politico Pro*, January 11, 2017.

[111] European Commission, "Report from the Commission to the European Parliament and the Council," COM(2018) 860 final, December 19, 2018.

the Privacy Shield is working and that the United States had made improvements and changes since the first review. The Commission, however, also noted areas of concern and specific recommendations.

General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (GDPR), effective May 2018, established rules for EU member states to safeguard individuals' personal data. 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. These measures have raised concerns about the GDPR's extraterritorial implications.

While the GDPR is directly applicable at the EU member state level, individual countries are responsible for establishing some national-level rules and policies as well as enforcement authorities, and some are still in the process of doing so. As a result, some U.S. stakeholders have voiced concern about a lack of clarity and inadequate country compliance guidelines, as well as about the potential high cost of data storage and processing needed for compliance. Despite the lack of precise guidance, many companies have taken steps to implement its requirements. For example, Amazon touts its compliance with GDPR requirements and aims to assist its Amazon Web Services (AWS) corporate customers, many of whom are small and medium businesses, with their own compliance.[112] It can be more challenging for SMEs to fully understand GDPR and comply with its notification and other requirements such as an individual's "right to be forgotten" and on data portability; there are indications that some U.S. businesses have chosen to exit the EU market.[113]

Some experts contend that the GDPR may effectively set new global data privacy standards, since many companies and organizations are striving for GDPR compliance to avoid being shut out of the EU market, fined, or otherwise penalized. In addition, some countries outside of Europe are imitating all or parts of the GDPR in their own privacy regulatory and legislative efforts. European Data Protection Authorities may have reinforced U.S. companies' concerns by initiating several enforcement actions in the fall of 2018, including a €50 million (approximately $57 million) fine on Google.[114]

Digital Single Market (DSM)

Like the GDPR, EU policymakers are attempting to bring more harmonization across the region through the Digital Single Market (DSM). The DSM is an ongoing effort to unify the EU market, facilitate trade, and drive economic growth. The DSM's three pillars revolve around better online access to cross-border digital goods and services; a regulatory environment supporting investment and fair competition; and driving growth through investment in infrastructure, human capital,

[112] See https://aws.amazon.com/compliance/gdpr-center/.

[113] "Websites not available in the European Union after GDPR," VerifiedJoseph.com, July 11, 2018, updated November 16, 2018, https://data.verifiedjoseph.com/dataset/websites-notavailable-eu-gdpr.

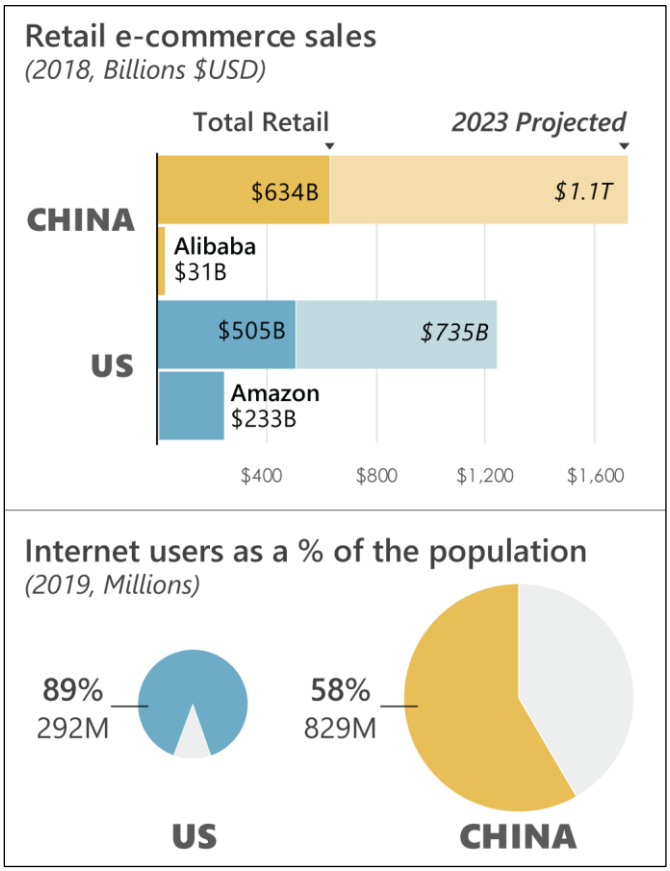
[114] For more information on GDPR, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick.

research, and innovation. Among its initiatives is a mandate to allow cross-border flows for nonpersonal data within the EU (with limited exceptions), but not necessarily externally.

China

China presents a number of significant opportunities and challenges for the United States in digital trade. The modernization 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. China's internet users grew from 21.5 million in 2000 to 829 million as of March 2019, and this trend will likely continue, given China's relatively low internet penetration rate (see **Figure 7**.)[115] China's online retail sales in 2018 totaled $1.1 trillion (more than double the U.S. level at $505 billion) and were the world's largest.[116] E-Marketer predicts that China's e-commerce retail sales will reach $1.99 trillion in 2019, accounting for 35.3% of total sales and 55.8% of global online sales.[117]

Figure 7. The U.S. and China Digital Trade Markets



Source: U.N. population statistics, Statista.com, Internetworldstats.com.

[115] *Internet World Statistics* at https://www.internetworldstats.com/top20.htm.

[116] Statista.com.

[117] E-Marketer, Newsroom, *2019: China to Surpass US in Total Retail Sales*, January 23, 2019, available at https://www.emarketer.com/newsroom/index.php/2019-china-to-surpass-us-in-total-retail-sales/.

U.S. firms may benefit from expanding digital trade in China, but they may also face numerous challenges in the Chinese market. The USTR's 2019 report on foreign trade barriers included a digital trade fact sheet that cited countries and practices of "key concern."[118] Three Chinese digital policies were listed, including its restrictions on cross-border data flows and data localization requirements; extensive web filtering and blocking of legitimate sites, including blocks 10 of the top 30 global sites and up to 10,000 sites in total, affecting billions of dollars in potential U.S. business; and cloud computing restrictions and requirements to partner with a Chinese firm to enter the market and to transfer technology and IP to the partner.[119]

The American Chamber of Commerce in China (AmCham China) 2019 business survey found that 73% of respondents who were engaged in technology and R&D-intensive industries stated that they faced significant or somewhat significant market barriers in China. The lack of sufficient IPR protection (cited by 35% of respondents) and restrictive cybersecurity-related policies (cited by 27% of respondents) ranked among the top three factors prohibiting firms from increasing innovation activities in China. The survey reflected significant concerns by member firms over eight Chinese ICT policies and restrictions (such as internet restrictions and censorship, IPR theft, and data localization requirements), with 72% to 88% of respondents stating that such measures impacted their competiveness and operations in China either somewhat or severely (see **Table 1**).

Table 1. AmCham China Business Survey: Percent of Respondents who said Certain Chinese IT Policies Affected their Operations and Competitiveness in China Somewhat or Severely

IT-related issues and practices	% of respondents
Slow cross border internet speed	88
Restricted access to online tools such as software	86
Cross-border internet access by virtual private networks (VPN)	83
Data security/IP leakage	79
Cybersecurity rules protecting critical information infrastructure/important data	75
Data privacy regulations	75
Internet censorship and restrictions on information publishing/sharing	73
Data localization requirements	72

Source: 2019 AmCham China Business Survey.

A Digital Trade Restrictiveness Index (DTRI) of 65 economies created by the European Centre for International Political Economy found China to have the most restrictive digital policies, followed by Russia, India, Indonesia, and Vietnam.[120] The index report noted:

[118] USTR, *Fact Sheet on 2019 National Trade Estimate: Key Barriers to Digital Trade*, March 2019, available at https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate.

[119] Examples of blocked sites include Google services (e.g., Gmail and YouTube), Twitter, Instagram, Facebook, the Washington Post, the New York Times, and the Wall Street Journal.

[120] The index was developed based on four factors: fiscal restrictions and market access, establishment restrictions, data restrictions, and trading restrictions. See

http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf

> China applies the most restrictive digital trade measures in many areas, including public procurement, foreign investment, Intellectual Property Rights (IPRs), competition policy, intermediary liability, content access and standards. The restrictions do not only impose higher costs for trading digital goods and services, they can also block digital trade altogether in certain sectors. In addition, China's data policies are extremely burdensome for companies, and the country also applies some quantitative trade restrictions and restrictions on e-commerce.[121]

Internet Governance and the Concept of "Internet Sovereignty"

The Chinese government has sought to advance its views on how the internet should be expanded to promote trade, but also to set guidelines and standards over the rights of governments to regulate and control the internet, a concept it has termed "Internet Sovereignty."[122] The Chinese government appears to have first advanced a policy of "Internet Sovereignty" around June 2010 when it issued a White Paper titled "the Internet of China," which stated the following:

> Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security.[123]

In 2014, the Chinese government established the Central Internet Security and "Informatization" Leading Group, headed by Chinese president Xi Jinping, to "strengthen China's Internet security and build a strong cyberpower." A year later, President Xi addressed an internet conference, stating "we should respect the right of individual countries to independently 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."[124]

Some analysts contend that China's internet sovereignty initiative represents an assertion that the government has the right to fully control the internet within China. Some see this as an attempt by the government to control information that is deemed a threat to social stability, in violation of the right to freedom of speech, which is guaranteed in China's Constitution. Other critics of China's internet sovereignty policy view it as an attempt by the government to limit market access by foreign internet, digital, and high technology firms in China, in order to boost Chinese firms and reduce China's dependence on foreign technology.

Cyber-Theft of U.S. Trade Secrets

China is considered by most analysts to be the largest source of global theft of IP and a major source of cybertheft of U.S. trade secrets, including by government entities. To illustrate, a 2011 report by the U.S. Office of the Director of National Intelligence (DNI) stated: "Chinese actors are the world's most active and persistent perpetrators of economic espionage. U.S. private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions

---

[121] The top five most open economies were New Zealand, Iceland, Norway, Ireland, and Hong Kong.

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

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

[124] Ministry of Foreign Affairs of the People's Republic of China, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*, December 16, 2015, available at http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

that have originated in China, but the IC (Intelligence Community) cannot confirm who was responsible." The report goes on to warn that

> China will continue to be driven by its longstanding policy of "catching up fast and surpassing" Western powers. The growing interrelationships between Chinese and U.S. companies—such as the employment of Chinese-national technical experts at U.S. facilities and the off-shoring of U.S. production and R&D to facilities in China—will offer Chinese government agencies and businesses increasing opportunities to collect sensitive US economic information.[125]

In May 2014, the U.S. Department of Justice issued a 31-count indictment against five members of the People's Liberation Army for cyber-espionage and other offenses that allegedly targeted five U.S. firms and a labor union for commercial advantage, the first time the Federal government had initiated such action against state actors.[126]

In April 2015, President Obama issued Executive Order 13964 authorizing certain sanctions against "persons engaging in significant malicious cyber-enabled activates."[127] This led to China sending a high-level delegation to Washington, DC, and, on September 25, 2015, Presidents Obama and Xi announced that they had reached an agreement on cyber-security and trade secrets that stated that neither country's government "will conduct or knowingly support cyber-enabled theft of IP, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[128] Specifically, the two sides agreed to

- Not conduct or knowingly support cyber-enabled theft of IP, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;
- Establish a high-level joint dialogue mechanism on fighting cybercrime and related issues;
- Work together to identify and promote appropriate norms of state behavior in cyberspace internationally; and
- Provide timely responses to requests for information and assistance concerning malicious cyber activities.[129]

The two sides also agreed to set up a high-level dialogue mechanism (which would take place twice a year) to address cybercrime and improve two-way communication when cyber-related concerns arise (including the creation of a hotline). The first meeting of the *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues* was held in December 2015. China and

[125] DNI, Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage*: 2009-2011, October 2011.

[126] U.S. Department of Justice, at http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[127] A copy can be found at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf. The EO was extended for an additional year by President Obama on March 29, 2016.

[128] The November 2015 meeting of the G-20 countries (which includes China) included this language in its communique: "In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

[129] The White House, Fact Sheet, President Xi Jinping's State Visit to the United States, September 25, 2015, available at https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

the United States reached agreement on a document establishing guidelines for requesting assistance on cybercrime or other malicious cyber activities and for responding to such requests. Two more meetings were held in 2016. The dialogue was continued in October 2017 under the Trump Administration.[130] The Administration's Section 301 trade dispute between the United States and China may have led to a suspension of the dialogue (see below).[131]

It is difficult to assess the effectiveness of the September 2015 U.S.-China cyber agreement in reducing the level of Chinese cyber intrusions against U.S. entities seeking to steal trade secrets as no official U.S. statistics on such activities are publicly available. In August 2018, the U.S. Deputy Director of the Cyber Threat Intelligence Integration Center stated that "the intelligence community and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral U.S.-China cyber commitments of September 2015."[132] In October 2018, CrowdStrike, a U.S. cybersecurity technology company, identified China as "the most prolific nation-state threat actor during the first half of 2018."[133] It found that Chinese entities had made targeted intrusion attempts against multiple sectors of the economy. In December 2018, U.S. Assistant Attorney General John C. Demers stated at a Senate hearing that from 2011-2018, China was linked to more than 90% of the Justice Department's cases involving economic espionage and two-thirds of its trade secrets cases.[134]

Cybersecurity Laws

According to the USTR's 2017 report on China's WTO accession, China has not fulfilled all of its WTO market opening commitments. The USTR cited "significant declines in commercial sales of foreign ICT products and services in China," as evidence that China continued to maintain "mercantilist policies under the guise of cybersecurity."[135]

The Chinese government pledged not to use recently enacted cyber and national security laws and regulations to unfairly burden foreign ICT firms, or to discriminate against foreign ICT firms in the implementation of various policy initiatives to promote indigenous innovation in China. Some Chinese laws or proposals include language stating that critical information infrastructure should be "secure and controllable," an ambiguous term that has not been precisely defined by Chinese authorities. Other proposals of concern to U.S. firms appear to lay out policies that would require foreign ICT firms to hand over proprietary information.

---

[130] See U.S. Department of Justice, *Press Release*, October 6, 2017, at https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

[131] The Diplomat, *Another US-China Dialogue Bites the Dust*, October 2, 2018, at https://thediplomat.com/2018/10/another-us-china-dialogue-bites-the-dust/.

[132] Office of the Director of National Intelligence, *Statement for the Record Mr. Michael Moss, Deputy Director Cyber Threat Intelligence Integration Center on "Cyber Threats to Our Nation's Critical Infrastructure,"* August 21, 2018, available at https://www.dni.gov/index.php/ctiic-newsroom/item/1899-statement-for-the-record-mr-michael-moss-for-confirmation-before-the-senate-select-committee-on-crime-and-terrorism-to-be-deputy-director-of-the-cyber-threat-intelligence-integration-center

[133] CrowdStrike, *CrowdStrike Report Reveals Cyber Intrusion Trends from Elite Team of Threat Hunters*, October 9, 2019, at https://www.crowdstrike.com/resources/news/crowdstrike-report-reveals-cyber-intrusion-trends-from-elite-team-of-threat-hunters/.

[134] U.S. Department of Justice, Statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice Before the Committee on the Judiciary, United States Senate, December 12, 2018, at https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf.

[135] USTR, *2017 Report to Congress on China's WTO Compliance*, January 2018, p. 3.

Examples of measures of concern to foreign ICT firms include

> **Cybersecurity Law**, passed by the government on November 7, 2016 (effective June 1, 2017), ascertains the principles of cyberspace sovereignty;[136] 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.[137]
>
> Some analysts have expressed concerns that one of the main goals of the new law is to promote the development of indigenous technologies and impose restrictions on foreign firms, and many multinational companies continue to voice concerns about the lack of clarity of the law's requirements, how the law will be interpreted and implemented through subsequent regulations, and to what extent it will impact their operations in China.

- **National Security Law**, enacted in July 2015, 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."[138]

Such restrictions could have a significant impact on U.S. ICT firms. According to BEA, U.S. exports of ICT services and potentially ICT-enabled services (i.e., services that are delivered remotely over ICT networks) to China totaled $18.7 billion in 2017.[139]

Section 301 Action against China over Intellectual Property and Innovation Issues

Concerns over China's policies on IP, technology, and innovation policies led the Trump Administration, in August 2017, to launch a Section 301 investigation of those policies.[140] 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, stating that China

[136] 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."

[137] 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.

[138] 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.

[139] See, BEA, *International Trade Data, U.S. Trade in Services*, https://apps.bea.gov/iTable/iTable.cfm?ReqID=62&step=1#reqid=62&step=1&isuri=1&6210=4.

[140] Sections 301 through 310 of the Trade Act of 1974, as amended, commonly referred to as "Section 301," procedures apply to foreign acts, policies, and practices that the USTR determines either (1) violates, or is inconsistent with, a trade agreement; or (2) is unjustifiable and burdens or restricts U.S. commerce, and sets procedures and timetables for actions based on the type of trade barrier(s) addressed.

1. Uses joint venture requirements, foreign investment restrictions, and administrative review and licensing processes to force or pressure technology transfers from American companies;
2. Uses discriminatory licensing processes to transfer technologies from U.S. companies to Chinese companies;
3. Directs and facilitates investments and acquisitions which generate large-scale technology transfer; and
4. Conducts and supports cyberintrusions into U.S. computer networks to gain access to valuable business information.

The USTR estimates such policies cost the U.S. economy at least $50 billion annually. Under the Section 301 action, the Administration proposed to (1) implement 25% ad valorem tariffs on certain Chinese imports (which in sum are comparable to U.S. trade losses); (2) initiate a WTO dispute settlement case against China's "discriminatory" technology licensing (which it did on March 23, 2018); and (3) propose new investment restrictions on Chinese efforts to acquire sensitive U.S. technology.[141] The Administration did not act on the last issue after Congress passed the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) (P.L. 115-232) in August 2018 to modernize the existing U.S. review process of foreign investments in terms of national security. Among its changes, FIRRMA expanded the types of investment subject to review, including certain noncontrolling investments in "critical technology."[142]

The Trump Administration subsequently imposed tariff hikes on $250 billion worth of imports from China in three separate stages in 2018, while China increased tariffs on $110 billion worth of imports from the United States (See **Figure 8**).[143] In May 2019, the United States increased the tariff levels on the third tranche of products imported from China. China subsequently increased its tariff levels on its third tranche.

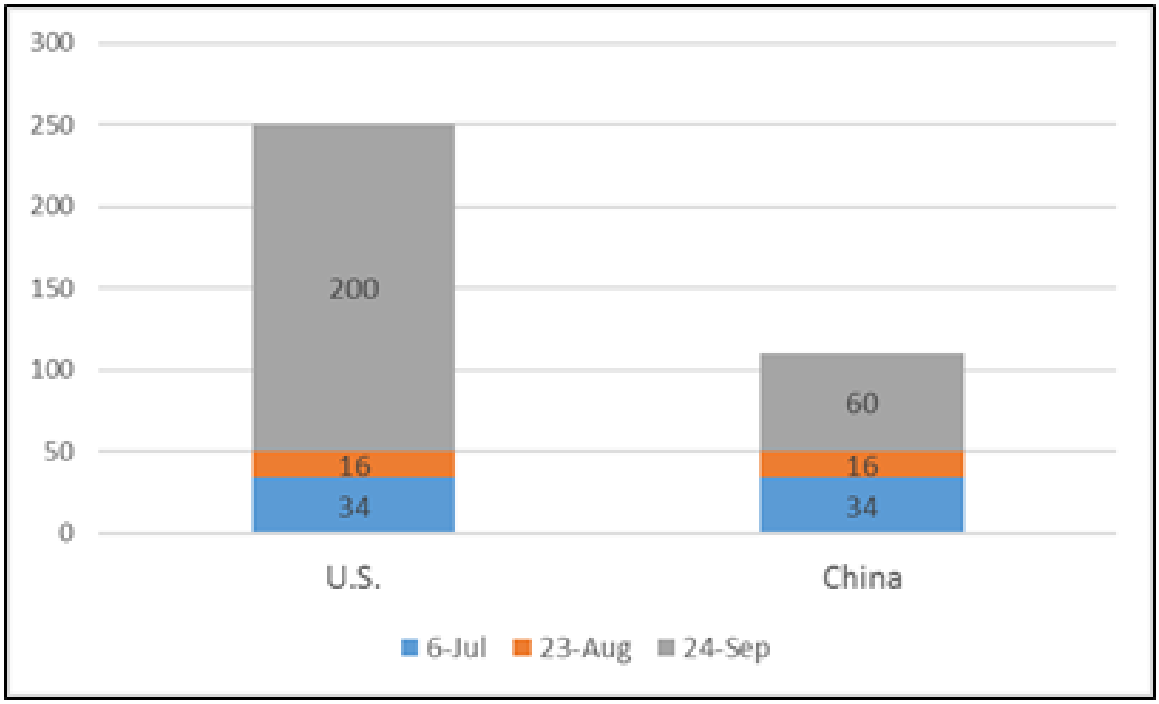
[141] For more information on the Section 301 investigation, see CRS In Focus IF10708, *Enforcing U.S. Trade Laws: Section 301 and China*, by Wayne M. Morrison.

[142] For more information on FIRMMA, see CRS In Focus IF10952, *CFIUS Reform: Foreign Investment National Security Reviews*, by James K. Jackson and Cathleen D. Cimino-Isaacs.

[143] These import hikes were as follows: 25% on $34 billion (July 6); 25% on $16 billion (August 23), and 10% on $200 billion (September 24). China's first two stages of retaliation matched U.S. levels in import and tariff levels while its third stage tariff hikes ranged from 5% to 10% on $60 billion worth of imports.

Figure 8. Three Rounds of U.S.-China Tariff Hikes in 2018

Estimated Value of Goods Impacted ($billions) and effective dates



Source: USTR and Chinese Ministry of Commerce.

Notes: Tariff rates vary.

Digital Trade Provisions in Trade Agreements

As the above analysis of EU and China policies demonstrates, there is not a single set of international rules or disciplines that govern key digital trade issues, and the topic is treated inconsistently, if at all, in trade agreements. As digital trade has emerged as an important component of trade flows, it has risen in significance on the U.S. trade policy agenda and that of other countries.

Given the stalemate in comprehensive WTO multilateral negotiations, trade agreements have 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).

WTO Provisions

While no comprehensive agreement on digital trade exists in the WTO, other WTO agreements cover some aspects of digital trade and new plurilateral negotiations may set new rules and disciplines.

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 the 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.[144]

As GATS does not distinguish between means of delivery, trade in services via electronic means is covered under GATS. While GATS contains explicit commitments for telecommunications and financial services that underlie e-commerce, digital trade and information flows and other trade barriers 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.[145]

Declaration on Global Electronic Commerce

In May 1998, WTO members established the "comprehensive" Work Programme on Electronic Commerce and established a temporary customs duties moratorium on electronic transmission that has been extended multiple times.[146] While multiple members submitted proposals to advance multilateral digital trade negotiations under the Work Programme, no clear path forward was identified.

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. The expanded ITA is a plurilateral agreement among 54 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 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. 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. The TRIPS Agreement does not specifically cover IPR protection and enforcement in the digital environment, but arguably has application to the digital

[144] 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.

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

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

environment and sets a foundation for IPR provisions in subsequent U.S. trade negotiations and agreements, many of which are "TRIPS-plus."

The TRIPS Agreement 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). TRIPS incorporates the main substantive provisions of WIPO conventions by reference, making them obligations under TRIPS. WTO members were required to fully implement TRIPS by 1996, with exceptions for developing country members by 2000 and least-developed-country (LDC) members until July 1, 2021, for full implementation.[147]

TRIPS aims to balance 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.[148]

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 has engaged in discussions on the agreement's relationship to electronic commerce as part of the WTO Work Programme on Electronic Commerce, focusing on protection and enforcement of copyright and related rights, trademarks, and new technologies and access to these technologies; new activity by the TRIPS Council to this end appears to be limited in recent years.[149]

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 WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty—often referred to jointly as the WIPO "Internet Treaties"—established international norms regarding IPR protection in the digital environment. These treaties were agreed to in 1996 and entered into force in 2002, but are not enforceable, including under WTO dispute settlement. Shaped by TRIPS, the WIPO Internet Treaties are intended to clarify that existing rights continue to apply in the digital environment, to create new online rights, and to maintain a fair balance between the owners of rights and the general public.[150]

---

[147] For pharmaceutical products, the implementation period has been extended until January 1, 2033.

[148] 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.

[149] WTO, General Council, "Item 6—Work Programme on Electronic Commerce—Review of Progress," WT/GC/W/701, July 24, 2015; and WTO, General Council, "Item 4—Work Programme on Electronic Commerce—Review of Progress," WT/GC/W/756, December 17, 2018.

[150] BSA, *Powering the Digital Economy: A Trade Agenda to Drive Growth*; and BSA, *Shadow Market: 2011 BSA Global Software Piracy Study*, May 2012.

Key features of the WIPO Internet Treaties include provisions for legal protection and remedies against circumventing 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). The liability of online service providers and other communication entities that provide access to the internet was contested in the negotiations on the WIPO Internet Treaties. In the end, WIPO Internet Treaties leave it to the discretion of national governments to develop the legal parameters for ISP liability.[151]

As of March 2019, the WIPO Internet Treaties had 96 contracting parties. The United States implemented the WIPO Internet Treaties through the Digital Millennium Copyright Act of 1998 (DMCA) (H.R. 2281), which set new standards for protecting copyrights in the digital environment, including prohibiting the circumvention of antipiracy measures incorporated into copyrighted works and enforcing such violations through civil, administrative, and criminal remedies.[152] The DMCA also, among other things, limits remedies available against ISPs that unknowingly transmit copyright infringing information over their networks by creating certain "safe harbors."[153] 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, such as Turkey and Mexico, to fully implement the WIPO Internet Treaties.[154]

WTO Plurilateral Effort

On the sidelines of the WTO Ministerial Conference, in December 2017, the United States, as part of a group of over 70 WTO members, agreed to "initiate exploratory work together toward future WTO negotiations on trade related aspects of electronic commerce."[155] The U.S. objectives include market access, data flows, nondiscriminatory treatment of digital products, protection of intellectual property and digital security measures, and intermediary liability, among others.[156]

The group formally launched the e-commerce initiative in January 2019.[157] The official joint statement lists includes advanced economies such as the United States, the EU, and Australia, 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.[158]

After the meeting, the U.S. Trade Representative's (USTR) statement emphasized the need for a high-standard agreement that includes enforceable obligations.[159] The EU noted e-signatures,

---

[151] 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.

[152] See P.L. 105-304.

[153] 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.

[154] USTR, *2017 Special 301 Report*, April 2017.

[155] WTO, "Joint Statement on Electronic Commerce," December 13, 2017, https://ustr.gov/sites/default/files/files/Press/Releases/Joint%20Statement%20on%20Electronic%20Commerce.pdf.

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

[157] WTO Joint Statement on Electronic Commerce, WT/L/1056, January 25, 2019.

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

[159] USTR, "USTR Robert Lighthizer on the Joint Statement on Electronic Commerce," January 25, 2019, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/january/ustr-robert-lighthizer-joint.

customs duties, forced disclosure of source code, and data localization measures among the potential new rules to be discussed.[160] Some analysts raise concerns that the EU may seek more limited commitments on issues such as cross-border data flows. China has proposed the negotiations be limited to exploratory discussions rather than establishing obligations on topics such as data flows and data storage.[161] The negotiating parties continue to discuss the scope of any potential agreement, but the outlook may be challenging given the different approaches and policies especially among the U.S., EU, and China.

U.S. Bilateral and Plurilateral Agreements

As traditional trade policy does not clearly reflect the pervasiveness of the digital economy, and data is increasingly incorporated into international trade, the line between goods and services, and the application of the existing multilateral trade agreement system, is not always clear. As discussed above, the WTO agreements provide limited treatment of some aspects of digital trade. The United States has sought to establish new rules and disciplines on digital trade in its bilateral and plurilateral trade negotiations.

Existing U.S. Free Trade Agreements (FTAs)

The United States has included an e-commerce chapter in its FTAs since it signed an agreement with Singapore in 2003 that has progressively evolved.[162] The e-commerce chapter of U.S. FTAs usually begins by recognizing e-commerce as an economic driver and the importance of removing trade barriers to e-commerce.[163] Most chapters contain provisions on nondiscrimination of digital products, prohibition of customs duties, transparency, and cooperation topics such as SMEs, cross-border information flows, and promoting dialogues to develop e-commerce. Some of the FTAs also include cooperation on consumer protection, as well as providing for electronic authentication and paperless trading. All FTAs allow certain exceptions to ensure that each party is able to achieve legitimate public policy objectives, protecting regulatory flexibility.

Electronic Commerce Chapter Article 1 in U.S. FTAs:

"The Parties recognize the economic growth and opportunity that electronic commerce provides, the importance of avoiding barriers to its use and development, and the applicability of the WTO Agreement to measures affecting electronic commerce."

The U.S.-South Korea FTA (KORUS) contains the most robust digital trade provisions in a U.S. FTA currently in force.[164] In addition to the provisions in prior FTAs, KORUS includes provisions on access and use of the internet to ensure consumer choice and market competition. Most significantly, KORUS was the first attempt in a U.S. FTA to explicitly address cross-border information flows. The e-commerce chapter contains an article that recognizes its importance and discourages the use of barriers to cross-border data but does not explicitly

[160] European Commission, "75 countries launch WTO talks on e-commerce," Press Release Database, January 25, 2019.

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

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

[163] 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.

[164] For more information on KORUS, see CRS Report RL34330, *The U.S.-South Korea Free Trade Agreement (KORUS FTA): Provisions and Implementation*, coordinated by Brock R. Williams.

mention localization requirements. The financial services chapter of KORUS also contains a specific, enforceable commitment to allow cross-border data flows "for data processing where such processing is required in the institution's ordinary course of business."[165]

In 2018, the Trump Administration and South Korea agreed to limited modifications of the agreement, but no changes were made to provisions directly impacting digital trade.

United States-Mexico-Canada Agreement (USMCA)

The released text of the proposed USMCA with Canada and Mexico aims to revise and update the trilateral North American Free Trade Agreement (NAFTA), and illustrates the Trump Administration's approach to digital trade.[166] The final text of the agreement pulls from and builds on many of the provisions from the Trans-Pacific Partnership (TPP) negotiated under President Obama which the United States did not ratify.[167] The provisions of the proposed USMCA establish new rules and disciplines to remove trade barriers and counter discriminatory action while also providing governments with flexibility. The provisions go much further than the KORUS agreement in establishing obligations on multiple aspects of digital trade, and contrast sharply with China's authoritarian approach discussed above.

USMCA provisions prohibit customs duties and discrimination against digital products, requirements for source code or algorithms disclosure, or technology transfer mandates. The agreement protects electronic authentication and signatures, electronic payment systems, and consumer access to the Internet. Provisions require anti-spam measures, domestic legal frameworks for online consumer and personal privacy protection, and identifies specific key principles and international guidelines that the parties must take into account. USMCA contains broad provisions to protect cross-border data flows and restrict data localization requirements; for financial services, open data flows is subject to the financial regulator having access to data necessary to fulfill its regulatory and supervisory role. The digital trade chapter also prohibits liability of internet intermediaries, in line with current U.S. law, and promotes the publication of government data through open-data formats. The parties agree to cooperate on and promote a number of issues including risk-based cybersecurity, privacy, SMEs, and the APEC Cross-Border Privacy Rules (see below).

Other International Forums for Digital Trade

Given the cross-cutting nature of the digital world, digital trade issues touch on other policy objectives and priorities, such as privacy and national security. 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 is ready, or willing, to take on such commitments. In other international forums outside of trade negotiations, other tools can be used to encourage high-level, nonbinding best practices and principles and align expectations.

[165] KORUS FTA, Chapter 13, Annex 13-B, Section B, https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file35_12712.pdf.

[166] The USMCA text is available at https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement.

[167] For more information on the TPP, see CRS In Focus IF10000, *TPP: Overview and Current Status*, by Brock R. Williams and Ian F. Fergusson.

G-20. The influential Group of 20 (G-20) is one venue for establishing common principles, and digital issues have been on its agenda recently.[168] At the 2017 meeting, G-20 leaders established the Digital Economy Task Force (DETF). The G-20 Digital Economy Ministerial Meeting issued a declaration that identified requisites for a thriving digital economy and specific recommendations.[169] As host, Japan is expected to build on the digital economy agenda in 2019, with a specific emphasis on privacy and data governance.

OECD. The OECD provides a forum to discuss principles and norms to facilitate a thriving digital economy. The OECD issued a series of reports in 2017 and 2018 related to digital trade, including an assessment of the digital transformation of each OECD economy[170] and bridging the digital gender divide.[171] The reports identified specific challenges and recommendations, including establishing a national digital strategy and removing market access barriers. The United States could work with its OECD partners to reinforce principles, including an open Internet and the need to balance public policy objectives. The OECD Global Forum on the Digital Security for Prosperity also allows for multi-stakeholder international engagement to discuss issues such as the governance of digital security issues.

APEC. The Asian Pacific Economic Cooperation (APEC) forum presents another opportunity for sharing best practices and setting high-level principles on issues that may be of greater concern to developing countries with less advanced digital economies and industry.[172] APEC is implementing the Cross-Border Privacy Rules (CBPR) system to be consistent with the already established APEC Privacy Framework.[173] According to the Business Software Alliance, most countries across the globe have data protection frameworks based on either the APEC CBPR system or the EU regime, but some countries still lack privacy laws.[174] Currently, the United States, Japan, Mexico, Canada, South Korea, Singapore, Taiwan, and Australia are CBPR members; the Philippines is in the process of joining. 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. Due to its voluntary nature, APEC has served as an incubator for potential plurilateral agreements.

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,

---

[168] 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). For more information on the G-20, see CRS Report R40977, *The G-20 and International Economic Cooperation: Background and Implications for Congress*, by Rebecca M. Nelson.

[169] https://g20.argentina.gob.ar/en/news/g20-confirms-importance-digital-economy-global-development.

[170] OECD, *Key Issues for Digital Transformation in the G20*, January 12, 2017, https://www.oecd.org/internet/key-issues-for-digital-transformation-in-the-g20.pdf.

[171] OECD, *Bridging the Digital Gender Divide: Include, upskill, innovate*, October 30, 2018, http://www.oecd.org/sti/ieconomy/bridging-the-digital-gender-divide.pdf.

[172] 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.

[173] http://publications.apec.org/Publications/2011/10/Enabling-Electronic-Commerce-The-Contribution-of-APECs-Data-Privacy-Framework.

[174] http://cloudscorecard.bsa.org/2018/index.html; http://cloudscorecard.bsa.org/2016/.

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

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

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 abroad, and trade negotiators who seek to open markets may focus on maintaining open market access, which may include cross-border data flows, while others may want to limit foreign competition. Privacy advocates may focus on protecting personal information. Meanwhile, law enforcement and defense advisors may seek the ability to access or limit information flows based on national security interests.

Digital trade raises numerous complex issues of potential interest to Congress with possible legislative and oversight implications. Issues include

- Understanding of the economic impact of digital trade on the U.S. economy and the effects of localization and other digital trade barriers on U.S. exports, jobs, and competition.
- Examining how best to balance market openness and cross-border data flows with other policy goals, such as right to privacy and the government's need for access to protect safety and national security.
- Considering if the United States would benefit from overarching digital privacy policy and what lessons can be drawn from other countries' experiences, and how to best balance this with U.S. trade negotiating objectives.
- Effectively addressing important digital trade barriers and cybertheft.
- Considering how best to assure public confidence and trust in network reliability and security that underlie the global digital economy and allow it to effectively and efficiently function.
- Examining evolving U.S. trade policy efforts, including how the proposed USMCA, WTO plurilateral, and potential new bilateral negotiations may address U.S. trade barriers, set new rules and disciplines, and respond to different standard-setting practices that may have global reach, including by the EU and China.
- Assessing if U.S. agencies have the necessary tools to accurately measure the size and scope of digital trade in order to analyze the impact of potential policies.
- Assessing the effectiveness of the Trump Administration's Section 301 actions involving Chinese trade practices and other bilateral efforts related to cybersecurity and digital trade.

Appendix. Digital Trade Barriers

Barriers to Internet Services

- Discriminatory treatment of digital goods and services
- Duties on digital goods or services
- Foreign investment restrictions
- Intermediary liability without safe harbor or fair-use provisions that could make internet platforms responsible for content posted by users
- Low de minimis threshold for customs duties on imported goods, including e-commerce purchases
- "Snippet tax" on search engines that quote text snippets as part of search results
- Taxes on over-the-top (OTT) services such as media, messaging, or voice-over-internet-protocol (VOIP)
- Web filtering and blocking of content

Localization Barriers

- Data localization requirements prohibiting cross-border data flows and requiring the use of local servers for data storage or processing
- Limited or no access to foreign government procurement markets
- Requirement for use of local technology
- Comprehensive privacy regulations that may discriminate against foreign providers

Technology Barriers

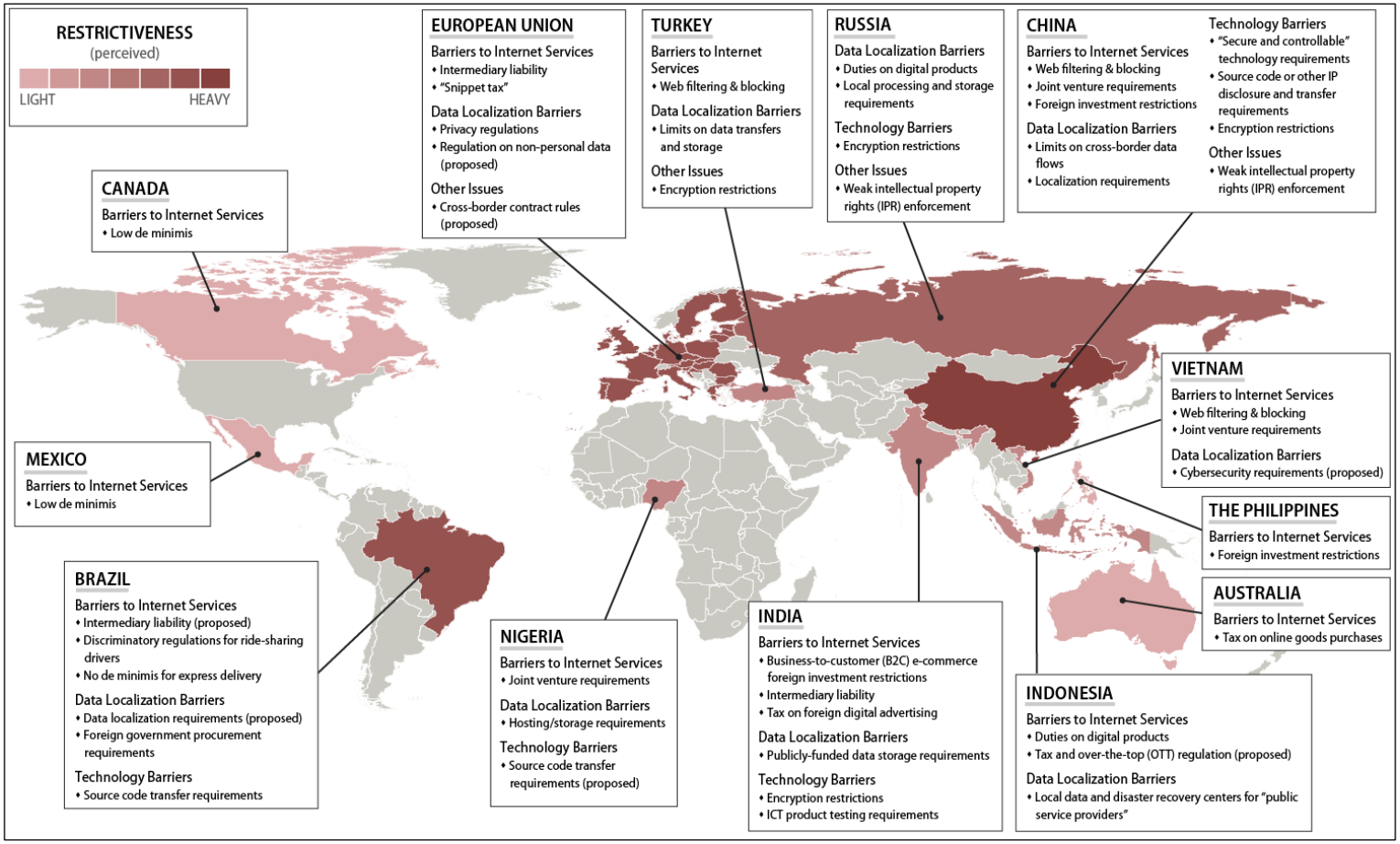
- Restrictions or prohibitions on use of encryption
- Source code, technology, or other intellectual property rights (IPR) forced transfer requirements
- Local testing and certification for imported information technology (IT) equipment may add costs or delays for imported goods

Other Barriers

- Cybersecurity threats or local requirements
- Weak IPR enforcement

Figure A-1. Levels of Perceived Digital Trade Barriers in Selected Countries

(according to the U.S. Trade Representative)



Source: CRS based on U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*.

Note: This map is illustrative of digital trade barriers and not meant to be an exhaustive list.

Author Information

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

Wayne M. Morrison
Specialist in Asian Trade and Finance

Shayerah Ilias 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.