Congressional Research Service
Informing the legislative debate since 1914

Digital Trade and U.S. Trade Policy

May 11, 2018

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. Growing faster than international trade or financial flows, the volume of global data flows grew 45-fold from 2005 to 2014.

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 2016, U.S. exports of information and communications technology-enabled services (excluding digital goods) were $404 billion. Digital trade is growing on a global basis; worldwide e-commerce was $27.7 trillion in 2016, up from $19.3 trillion in 2012.

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, 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 renegotiation of the North American Free Trade Agreement (NAFTA) and the potential plurilateral Trade in Services Agreement (TiSA) 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 11
Nontariff Barriers 12
Localization Requirements 13
Intellectual Property Rights (IPR) Infringement 15
National Standards and Burdensome Conformity Assessment 17
Filtering, Blocking, and Net Neutrality 17
Cybersecurity Risks 18
U.S. Digital Trade with Key Trading Partners 19
European Union 19
EU-U.S. Privacy Shield 22
General Data Protection Regulation (GDPR) 22
Digital Single Market (DSM) 23
China 24
Internet Governance and the Concept of "Internet Sovereignty" 24
IP Theft 26
Digital Trade Provisions in Trade Agreements 29
WTO Provisions 30
General Agreement on Trade in Services (GATS) 30
Declaration on Global Electronic Commerce 30
Information Technology Agreement (ITA) 31
Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 32
World Intellectual Property Organization (WIPO) Internet Treaties 32
U.S. Bilateral and Plurilateral Agreements 33
Existing U.S. Free Trade Agreements (FTAs) 33
Trans-Pacific Partnership (TPP) Agreement 34
North American Free Trade Agreement (NAFTA) 35
Trade in Services Agreement (TiSA) Negotiations 36
Other International Forums for Digital Trade 36
Issues for Congress 38

Figures

Figure 1. Growth in Global Trade, Finance, and Data Flows 2
Figure 2. A Typical Day in the Life of the Internet 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. U.S.-China High-Level Joint Dialogues on Cybercrime and Related Issues 27

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

Appendixes

Appendix. Digital Trade Barriers 39

Contacts

Author Information 41
Acknowledgments 41

Introduction

The internet-driven digital revolution is causing fundamental change to the U.S. and global economy, leading not only to new modes of communication and information-sharing, business models, and sources of job growth, but also to new policy challenges. Data and data flows form the foundation for innovation and engine of economic growth. Almost two-thirds of jobs created in the United States since 2010 required medium or advanced levels of digital skills.[1] 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).[2]

Digital trade includes not only end-products like downloaded movies and video games, but also the means to enhance the productivity and overall competitiveness of an economy, such as information streams needed by manufacturers to manage global operations; communication channels (email and voice over internet protocol [VoIP]); and financial data and transactions for online purchases or electronic banking.

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 ongoing renegotiation of the North American Free Trade Agreement (NAFTA). 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.

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

---

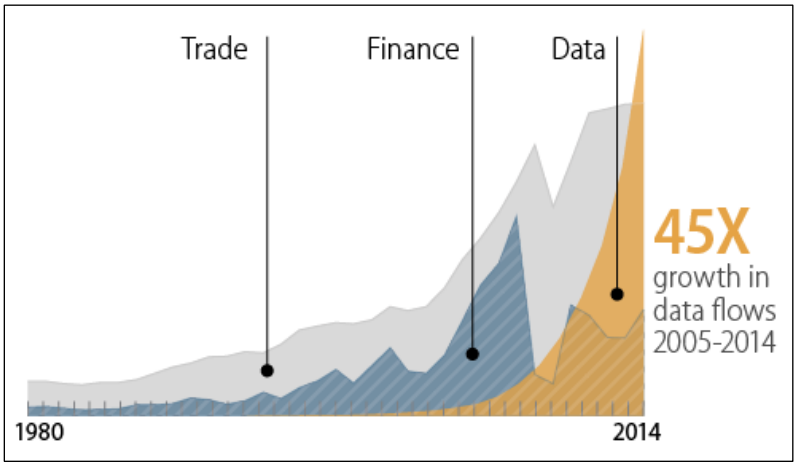
[1] Penny Pritzker and John Engler, Director Edward Alden, *The Work Ahead: Machines, Skills, and U.S. Leadership in the Twenty-First Century, Independent Task Force Report*, The Council for Foreign Relations, April 2018.

[2] 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.

Role of Digital Trade in the U.S. and Global Economy

The internet not only has become a facilitator of existing 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 is growing faster than trade or financial flows (see **Figure 1**). Some analyses indicate that global flows of goods, services, finance, and people increased gross domestic product (GDP) by at least 10% in the past decade, adding U.S. $8 trillion by 2015.[3]

Figure 1. Growth in Global Trade, Finance, and Data Flows



Source: McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, March 2016.

The increase in digital trade parallels the growth in internet usage globally. According to the United Nations International Telecommunication Union (ITU), 48% of people globally use the internet.[4] The Organisation for Economic Co-operation and Development (OECD) reports that in 2014, on average, 95% of enterprises in OECD countries had a broadband connection and 76% had a website or homepage.[5] In the United States, 92% of the population uses the internet, according to one estimate.[6] While 75% of U.S. households use wired internet access, an increasing number are relying on mobile internet access, with 72% of U.S. adults owning a smartphone, as the internet is integrated into people's everyday lives.[7] While the percentage of American consumers relying on a desktop or laptop at home is declining, they increasingly are turning to an array of devices from smartphones to wearable devices for internet access.[8] Each

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

[4] ITU, *ICT Facts and Figures 2017*, 2017, http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

[5] The United States was not included in the study. OECD. (2015), "Executive summary," *OECD Digital Economy Outlook 2015*, pp. 2-3, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264232440-2-en.

[6] Internet Association, *Measuring the U.S. Internet Sector*, 2015, http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

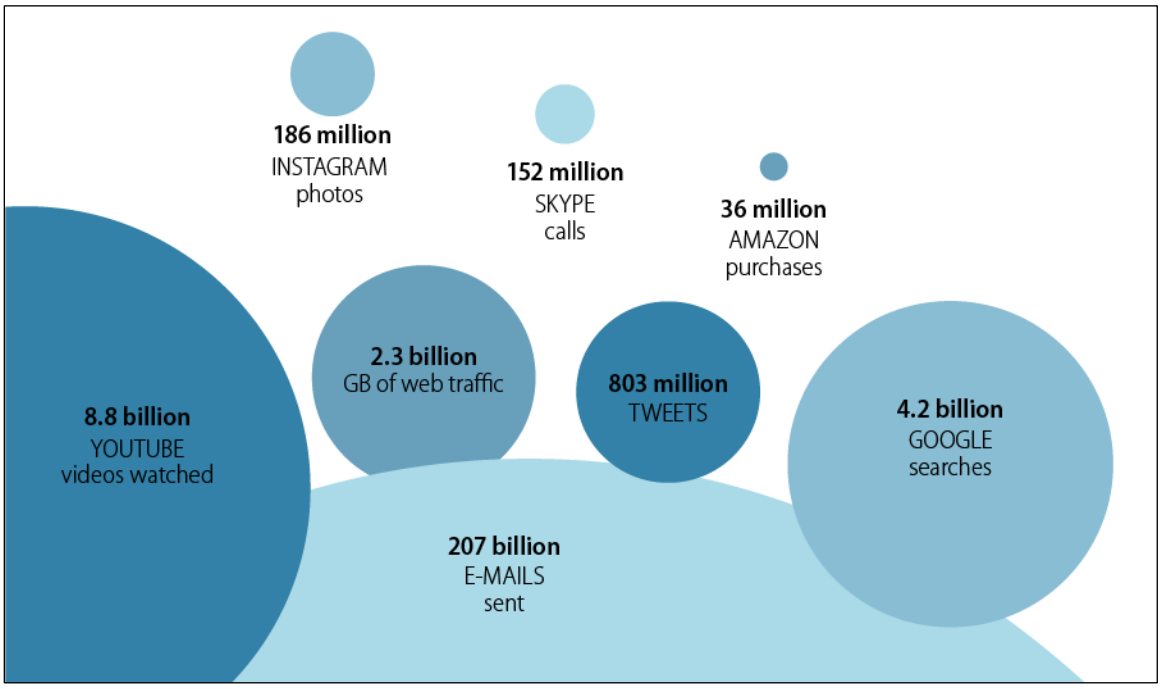
[7] U.S. International Trade Commission, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, Publication Number: 4716, Investigation Number: 332-561, August 2017, p.47-49, https://www.usitc.gov/publications/332/pub4716.pdf.

[8] Giulia McHenry, *Evolving Technologies Change the Nature of Internet Use*, National Telecommunications &

day, companies and individuals depend on the internet to communicate and transmit data via various media and channels that continue to expand with new innovations (see **Figure 2**).

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. One estimate shows that although cross-border bandwidth grew by 45 times from 2005 through 2015, it may grow by nine times more by 2021.[9] 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 impact digital trade, which could decrease efficiency and other potential benefits.

Figure 2. A Typical Day in the Life of the Internet



Source: The World Bank Group, World Development Report 2016: Digital Dividends, 2016, p. 6, http://www.worldbank.org/en/publication/wdr2016.

Powering all these connections and data flows are underlying information and communication technologies (ICT).[10] ICT spending is a large and growing component of the international economy and essential to digital trade and innovation. For example, software contributed more than $1.14 trillion to the U.S. value-added 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.[11]

According to the OECD, world trade in ICT physical goods grew 12% from 2008 through 2015. In the United States, growth in ICT manufacturing output was approximately 5% per year as of

Information Administration blog, April 19, 2016.

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

[10] 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.

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

2015-2016.[12] The broader digital sector (defined as online platforms, platform-enabled services, and suppliers of ICT goods and services) accounted for approximately 1% in 2015.[13] Semiconductors, a key component in many electronic devices, are a top U.S. ICT export, and global sales of semiconductors grew to $412.2 billion in 2017, an increase of 21.6% over the prior year.[14] Given the importance of semiconductors to the digital economy, 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. A U.S. competitive strength, the United States is the fourth-largest OECD exporter of ICT services, after Ireland, India, and the Netherlands.[15] 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 2016, exports of ICT services accounted for $66 billion of U.S. exports while services exports that could be potentially ICT-enabled were another $404 billion, demonstrating the impact of the internet and digital revolution.[16]

[12] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, p. 120-124. http://dx.doi.org/10.1787/9789264276284-en.

[13] OECD, Measuring the Digital Economy, OECD Staff Report, February 2018.

[14] Semiconductor Industry Association, "Annual Semiconductor Sales Increase 21.6 Percent, Top $400 Billion for First Time," February 5, 2018.

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

[16] Bureau of Economic Analysis (BEA), https://www.bea.gov/iTable/iTable.cfm?ReqID=62&step=1#reqid=62&step=9&isuri=1&6210=4.

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.

According to USITC estimates, digital trade, including both U.S. domestic commerce and international trade, increased U.S. GDP by an estimated 3.4%-4.8% ($517.1-$710.7 billion) in 2011. In addition, U.S. real wages increased by an estimated 4.5%-5.0% and total U.S. employment was higher by 2.4 million full-time equivalents (FTEs) as a result of digital trade.[17] Some estimates show that, without the internet, the costs of U.S. imports and exports would have been an average of 26% higher, potentially lowering profits or increasing end prices.[18]

Looking at digital trade in an international context, approximately 12% of physical goods are traded via international e-commerce.[19] Global e-commerce grew from $19.3 trillion in 2012 to $27.7 trillion in 2016, of which 86% was business-to-business (B2B).[20] One study found that over half of internet users globally purchased online in 2015.[21]

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. 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.[22] Their analysis showed that the long-term return on investment (ROI) for digital technologies is 6.7 times that of nondigital investments.[23]

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.[24] For example, in an effort to streamline processes, save costs, and improve public health outcomes, Walmart and IBM are piloting a blockchain platform to increase transparency of global supply chains and improve traceability for certain imported food products.[25] 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

[17] U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, Publication No: 4485, Investigation No: 332-540, p. 13, August 2014, https://www.usitc.gov/publications/332/pub4485.pdf.

[18] 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, p. 65, https://www.usitc.gov/publications/332/pub4485.pdf.

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

[20] 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.

[21] eMarketer,"Worldwide Retail E-commerce Sales: eMarketer's Updated Estimates and Forecast Through 2019," https://www.emarketer.com/public_media/docs/eMarketer_eTailWest2016_Worldwide_ECommerce_Report.pdf.

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

[23] Ibid.

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

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

applications, the Internet of Things may have a global economic impact of as much as $11.1 trillion per year, according to one study.[26]

What Is the Internet of Things and Blockchain?

Internet of Things

"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."[27]

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)."[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) (see **text box**).

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.[32] With simpler border and customs processes, more firms are able to conduct business in global markets (or are more willing to do so). A study of U.S. SMEs on the e-

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

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

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

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

commerce platform eBay found that 97% export, while that number is a full 100% in countries as diverse as Peru and Ukraine.[33]

Example of a Local Company Expanding Due in Large Part to Digital Trade

TSheets cofounders Matt Rissell and Brandon Zehm created an internet cloud-based, employee-time-tracking solution that worked with QuickBooks. Started in 2006, the company has since hired 60 employees, expanded into 63 countries, and was named Idaho's Innovative Company of the Year by the Idaho Technology Council. The company uses Google services for online advertising and customer engagement, analytics, document storage, and to enhance their own products. "Because of the Internet and the tools available to us, we've been able to grow an international company based in Boise, Idaho," Matt says.[34]

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."[35] 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.[36] However, the costs of digital trade can be concentrated on particular sectors (see next section).

Digitization Challenges

Software, and the software industry, is adding to the GDP in all 50 states, with Idaho and North Carolina growing more than 40% due to software.[37] However, the U.S. economy may only be realizing 18% of its digital potential, and it is doing so unevenly across sectors and populations.[38] Industries, such as media and those 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. Some experts estimate digitization could add another $2.2 trillion a year to the U.S. GDP by 2025.[39]

Additionally, sources of "e-friction" or obstacles can prevent consumers, companies, and countries from realizing the full benefits of the online economy.[40] Causes of e-friction can fall

[33] 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.

[34] Google President Margo Georgiadis, *Economic Impact United States 2014*, p. 20, https://static.googleusercontent.com/media/www.google.com/en//economicimpact/reports/2014/ei-report-2014.pdf.

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

[36] 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.

[37] Software.org, "The Growing $1 Trillion Economic Impact of Software."

[38] Digital potential is defined as the upper bounds of digitization in the leading sectors included in the study. 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. 32, http://www.mckinsey.com/industries/high-tech/our-insights/digital-america-a-tale-of-the-haves-and-have-mores.

[39] Ibid.

[40] Paul Zwillenberg, Dominic Field, and David Dean, *Greasing the Wheels of the Internet Economy*, Boston Consulting

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.[41]

While there are numerous positive digital dividends, there are also potential negative and uneven results across populations, such as the displacement of unskilled workers, an imbalance between companies with and without internet access, and potential for some to use the internet to establish monopolies.[42] 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.[43]

The World Bank identified policy areas 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 Competitiveness Rankings, which looks at technological adoption and ICT use, the United States is ranked 17th.[44] 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.[45] Over two-thirds of U.S. jobs created since 2010 require some level of digital skills.[46] The OECD found that generic ICT skills are insufficient among a significant percentage of the global workforce and few countries have adopted comprehensive ICT skills strategies to help workers adapt to changing jobs.[47]

Group, February 2014, https://www.bcgperspectives.com/content/articles/digital_economy_telecommunications_greasing_wheels_internet_economy/.

[41] Ibid.

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

[43] 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.

[44] World Economic Forum; Global Competitiveness Report 2015-2016; date of data collection or release: September 1, 2015, http://www.weforum.org/gcr.

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

[46] 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.

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

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 AppendixXXX.

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.[48]

Ensuring a free and open internet is a stated policy priority for the U.S. government.[49] 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.[50]

Protect a Free and Open Internet[51]

Protecting a free and open internet is a policy priority as stated in President Trump's *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:[52]

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";

[48] 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.

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

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

[51] 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.

[52] 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.

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."

The Commerce Secretary launched specific efforts to support the Digital Economy Agenda, including a Digital Economy Board of Advisors from across sectors[53] and a pilot digital attaché program under the foreign commercial service to help U.S. businesses navigate regulatory issues and overcome trade barriers to e-commerce exports.[54]

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-$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.[55]

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.[56] Congress recognized the importance of digital trade and removing related barriers when it passed TPA. 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.

[53] U.S. Department of Commerce, "Digital Economy Board of Advisors Membership Balance Plan," January 3, 2018, https://www.ntia.doc.gov/files/ntia/publications/deba_membership_balance_plan-1-3-2018.pdf.

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

[55] 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.

[56] 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.

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.[57]

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,[58] despite tariffs of up to 16% on these products.[59]

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.[60] 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.[61]

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.

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
- Cybertheft of U.S. trade secrets
- Forced technology transfer

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

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.

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

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

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

[60] U.S. Census Bureau.

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

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.[62] Governments often use privacy 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 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.[63] 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.[64]

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, 70% of all 2015 global internet traffic went through cloud data centers compared to 30% in 2011, and approximately 40% of those cloud data center workloads were in North America.[65] In 2014, 22% of businesses in OECD member countries used cloud computing services, with higher use among large enterprises, and the number is accelerating.[66] Most of the largest global providers of cloud computing services are U.S. companies (Amazon, Microsoft, Google, and IBM).

---

[62] 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.

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

[64] 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.

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

[66] OECD. (2015), "Executive summary," *OECD Digital Economy Outlook 2015*, p. 5, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264232440-2-en.

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 EU, Indonesia, South Korea, Russia, and Vietnam.[67] The Business Software Alliance's 2018 Global Cloud Computing Scorecard highlighted barriers to cloud services in Indonesia, Russia, and Vietnam.[68] 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.[69]

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."[70] 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.[71]

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 original equipment manufacturers (OEMs) in Nigeria to assemble all hardware products locally and multinational companies operating in Nigeria to source all ICT hardware locally.
- In **India**, the 2015 National Telecom M2M ("machine to machine") roadmap recommends preferences for locally manufactured SIM cards and domestically sourced goods, and requirements that application servers and gateways that serve customers in India be located domestically.

Source: 2018 National Trade Estimate Report on Foreign Trade Barriers, Office of the United States Trade Representative, 2018.

[67] 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.

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

[69] Google Cloud Platform Blog, "Google Cloud Platform adds two new regions, 10 more to come," March 22, 2016, https://cloudplatform.googleblog.com/2016/03/announcing-two-new-Cloud-Platform-Regions-and-10-more-to-come_22.html?mod=djemCIO_h.

[70] 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.

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

Intellectual Property Rights (IPR) Infringement

Intellectual property rights (IPR)[72] are legal, private, enforceable rights that governments grant to inventors and artists; they generally provide rights holders with time-limited monopolies over the use of their creations, enabling them to exclude others from using their creations without their permission. IPR come in a variety of forms, such as patents, copyrights, trademarks, and trade secrets. While they are intended to encourage innovation and creative output by allowing inventors and artists to reap the benefits of the time and money they direct to developing IP, the rights are time-limited so that other inventors and artists can build on them and society can benefit more broadly through wider availability of works.

A wide range of U.S. industries rely on IPR protection. According to the Department of Commerce, IP-intensive industries accounted for about $6.6 trillion in value added, or 38.2% of U.S. gross domestic product (GDP) in 2014.[73] These industries also were estimated to account for $842 billion (or 52% of) U.S. merchandise exports in 2014; and $81 billion (or 12.3% of) U.S. private services exports in 2012.[74] In 2016, U.S. charges for the use of IP (i.e., receipts of royalties and license fees) totaled about $124 billion, representing 16% of U.S. services exports, while U.S. payments for the use of IP (i.e., payments of royalties and license fees) totaled about $44 billion, representing about 9% of U.S. services imports.[75] Given the role of IP in the U.S. economy, IPR infringement presents significant trade and economic concerns for U.S. policymakers (see **text box**).

How Much IPR Infringement?

By its nature, IPR infringement is difficult to quantify, and quantifying such infringement in the digital environment is all the more challenging given that, for example, "infringing files are traded online and websites offering counterfeits are launched and accessed, countless times each day."[76] According to USTR, online sales of pirated and counterfeit goods reportedly could exceed the volume of sales "through traditional channels such as street vendors and other physical markets." A 2016 International Chamber of Commerce (ICC) study estimated the value of digitally pirated music, movies, and software (not actual losses) as $213 billion in 2013 to potentially $384-$856 billion in 2022.

Sources: USTR, *2017 Special 301 Report*, April 2017; 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), June 2017.

While the internet and digital technologies have opened up markets for international trade, they also have raised challenges of IPR infringement (e.g., theft of IP, such as copyright piracy or counterfeiting of trademarks). Innovations in digital technologies fuel IPR infringement by enabling the rapid duplication and distribution of content that is low-cost and high-quality,

[72] Intellectual property is a creation of the mind—such as an invention, literary/artistic work, design, symbol, name, or image—embodied in a physical or digital object. 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 Akhtar and Ian F. Fergusson.

[73] U.S. Department of Commerce, *Intellectual Property and the U.S. Economy: 2016 Update*, prepared by the Economics and Statistics Administration and the U.S. Patent and Trademark Office, 2016.

[74] Ibid.

[75] CRS, based on U.S. Bureau of Economic Analysis (BEA), Table 2.1. U.S. Trade in Services, by Type of Service,, *Survey Of Current Business*, October 2017. The charges for the use of IP reflect those not included elsewhere in BEA services data.

[76] ITC, *Digital Trade in the U.S. and Global Economies, Part 1*, USITC Publication 4415, July 2013, p. 5-15.

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."[77] IPR enforcement in the digital environment raises particular challenges.[78]

Efforts to address IPR infringement raise issues of balance about, on one hand, protecting and enforcing IPR to incentivize innovation and, on the other hand, setting appropriate limitations and exceptions to ensure other economically and socially valuable uses. U.S. stakeholders differ on how to address such issues. Representatives of "content" industries have singled out internet-enabled piracy as the most important barrier to digital trade for their industries (see **text box**). Barriers include foreign websites that facilitate IPR infringement, such as through hosting pirated content or connecting users to such content. Cybertheft of trade secrets presents additional, increasingly prominent, barriers to digital trade.[79] Content industries say that IP theft costs them sales, takes away from legitimate services, harms investors in these businesses, damages their brand or reputation, and hurts "law-abiding" consumers.[80]

Examples of IPR Infringement in Digital Trade

- **Foreign websites that facilitate IPR infringement.** Some foreign websites offer large platforms to distribute globally infringing content (e.g., unauthorized copies of music, movies, software, video games) and illicit physical goods (e.g., counterfeit drugs). These websites take a variety of forms, including auction, business-to-business, consumer-to-consumer, and business-to-consumer sites. Some operate as "hubs" that allow users to upload content to file-sharing websites ("cyberlockers"), search applications that connect to websites to access content illegally (such as "e-libraries"), streaming sites that provide unauthorized access to copyrighted materials (such as "camcorded" copies of movies, and retransmission of live sports programs), and "pirate servers" that allow users to run unauthorized versions of cloud-based software. The USTR *2016 Notorious Markets* report highlights a number of countries in which parties host or operate online markets believed to be engaged in or facilitating substantial IPR infringement; these include Brazil, Canada, China, the Netherlands, Russia, Switzerland, Ukraine, and Vietnam.
- **Software piracy.** Issues include "end-user" piracy of software (e.g., installing software on multiple computers beyond license terms) and unauthorized installation of software, movies, music, and other creative programming.
- **Circumvention of technological protection measures (TPMs).** Measures such as encryption intend to limit the unauthorized reproduction, transmission, and use of products. Development and online distribution of devices that allow for TPM circumvention (e.g., modchips that allow users to play pirated games on physical consoles) raise IPR concerns.
- **Cybertheft of trade secrets.** Theft of trade secrets, including through cybertheft (e.g., cyberintrusions and hacking), appears to be escalating. Trade secrets are essential to many businesses' operations and important assets, including those in ICT, services, biopharmaceuticals, manufacturing, and environmental technologies.
- **Trademark infringement related to domain names.** Lack of protection of trademarks against unauthorized uses under country code top level domain names (ccTLDs) and "cybersquatting" is a concern for IPR-based businesses, and is related to the loss of internet traffic. The ccTLDs in China and several European countries are among those identified as presenting issues.

Sources: USTR, *2017 Special 301 Report*, April 2017; USTR, *2016 Notorious Markets List*, December 2016; and ITC, *Digital Trade in the U.S. and Global Economies, Part 1*, USITC Publication 4415, July 2013.

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

[78] For example, the USTR *2016 Notorious Markets* report highlights several foreign websites involved in or facilitating substantial piracy and counterfeiting that continue to operate despite being subject to law enforcement action. See USTR, *2016 Out-of-Cycle Review of Notorious Markets*, December 2016.

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

[79] ITC, *Digital Trade in the U.S. and Global Economies, Part 1*, USITC Publication 4415, July 2013, p. 5-1.

[80] Ibid., pp. 5-15.

Some technology product and service companies, as well as some civil society groups, also assert that overly stringent IPR policies may stifle information flows and legitimate digital trade. Thus, they support exceptions and limitations to IPR, such as for "fair use"—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.

For example, the USTR cites concerns regarding proposals for mandatory fees in the EU for linking to content published online, efforts that the USTR says appear to be targeting particular news aggregators that "index and allow users to more conveniently find and access such content by the inclusion in search results of headlines or other extracts of the stories that the underlying publisher typically offers, without charge (e.g., supported by advertising) on its own website."[81]

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.[82] If a company is required to provide the source code, proprietary algorithms, or other IP to gain market access, it may fear theft of its IP and not enter that market (see above).

Filtering, Blocking, and Net Neutrality

In some nations, government seeks strict control over digital data within its borders, such as what information people can access online, and how information is shared inside and outside its borders. 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

[81] USTR, *2017 National Trade Estimate Report on Foreign Trade Barriers*, p. 181-2, March 2017.

[82] *2018 National Trade Estimate Report on Foreign Trade Barriers*, Office of the United States Trade Representative, 2018, p. 219.

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).[83]

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.[84] In Russia, citizens protested government censorship, including the blocking of a popular messaging application along with other websites and online tools.[85]

Due to the global nature of the internet, one nation's preferences or regulations can have spillover effects on the rest of the world. French privacy authorities, for example, fined Google $112,000 for not applying a ruling on the "right to be forgotten" and deleting certain content across the company's domains worldwide.[86] While Google had adopted the ruling by the Court of Justice of the European Union (CJEU) across all of its European operations, it had not done so globally, given that there is no one international standard or policy it is required to comply with. These types of challenges may increase with the implementation of the EU General Data Protection Regulation (see "General Data Protection Regulation (GDPR)"). The conflict between Google and the EU authorities illustrates 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.[87] In the United States, the Federal Communications Commission (FCC) classification of broadband internet service providers (ISPs) has been controversial domestically and may differ from how U.S. trading partners regulate ISPs.

Cybersecurity Risks

The growth in digital trade has raised issues related to cybersecurity, the act of protecting ICT systems and their contents from cyberattacks. Cyberattacks in general are deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Cybersecurity can also be an important tool in protecting privacy and preventing unauthorized surveillance or intelligence gathering.[88] 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.[89]

---

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

[84] *2018 National Trade Estimate Report on Foreign Trade Barriers*, Office of the United States Trade Representative, 2018, p. 446.

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

[86] Mark Scott, "Google Fined by French Privacy Regulator," *The New York Times*, March 24, 2016.

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

[88] 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.

[89] Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, February 2018,

Cyberattacks can pose broad risks to financial and communication systems, national security, privacy, and digital trade and commerce. 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.[90]

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.[91] 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."[92]

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.[93] However, restrictions on the ability for a firm to use encryption may make a company vulnerable to cyberattacks or cybertheft, demonstrating the need for policies and regulations to balance competing objectives.

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. The United States and EU trade $2.7 billion a day worth of goods and services, and the annual digital services trade between the two regions is approximately $260 billion.[94] The two sides also account for a significant portion of each other's e-commerce trade (see **Figure 4**).

---

https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

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

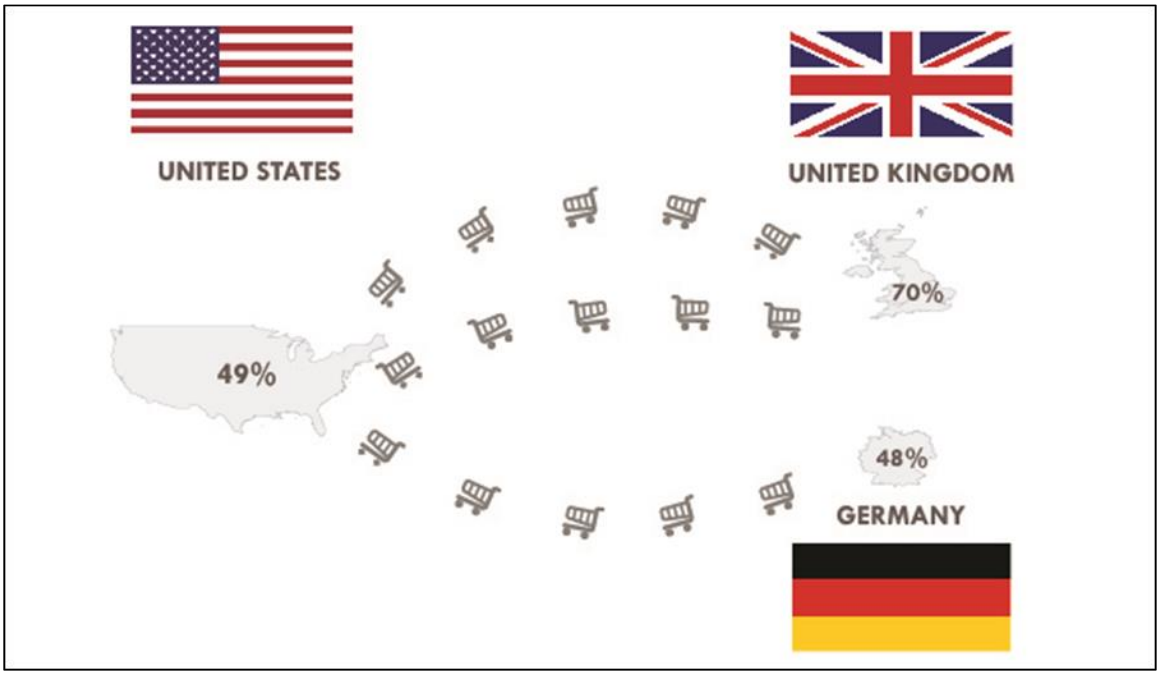
[91] Nick Kostov, Jeannette Neumeann, and Stu Woo, "Cyberattack Victims Begin to Assess Financial Damage," *Wall Street Journal*, May 14, 2017.

[92] 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.

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

[94] Penny Pritzker, Former U.S. Secretary of Commerce and Andrus Ansip, Vice-President of the European Commission for the Digital Single Market, "Making a Difference to the World's Digital Economy: The Transatlantic Partnership," March 11, 2016, https://www.commerce.gov/news/blog/2016/03/making-difference-worlds-digital-economy-transatlantic-partnership.

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.

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.

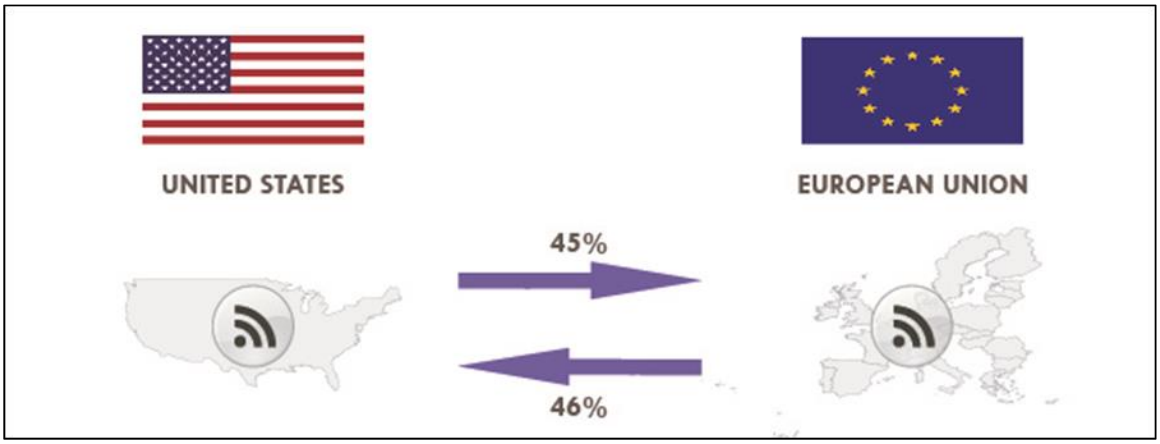
The United States and EU account for almost half of each other's digitally deliverable service exports (e.g., business, professional, and technical services) and many of these services are incorporated into exported goods as part of GVCs (see **Figure 5**and **Figure 6**).[95] The UK alone accounted for 23% of U.S. digitally deliverable services exports.[96] Almost 40% of the data flows between the United States and EU are through business and research networks.[97]

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

[96] Ibid.

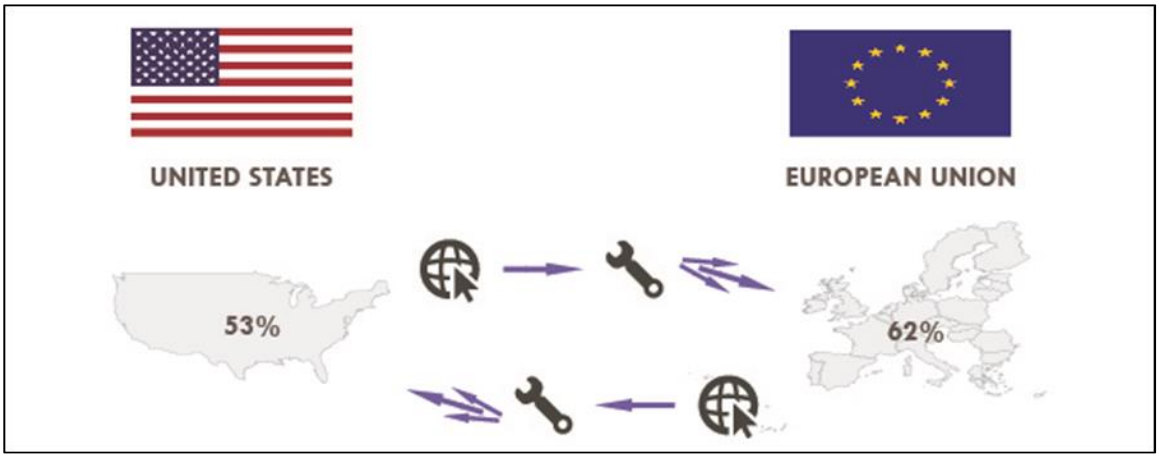
[97] All figures on U.S.-EU trade and data flows includes the United Kingdom (UK) as part of the EU. Without the UK, the statistics would be lower.

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 negotiating a broad FTA to reduce and eliminate tariff and nontariff barriers on goods, services, and agriculture, as well as to establish globally relevant trade rules and disciplines that expand on WTO commitments and address newer issues such as digital trade. 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.[98] While the broader FTA negotiations are paused under the Trump Administration, digital trade is affected by other ongoing U.S. and EU initiatives and may be a focal point in any potential future negotiations between the United States and UK.

[98] 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.

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.[99] 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 U.S.-EU agreement.[100]

The Privacy Shield also involves an annual joint review by the United States and the EU, the first of which was completed in October 2017.[101] Under the review, the commission found that the Privacy Shield is working but identified a list of recommendations for improvement, including asking Congress to incorporate the protections offered by Presidential Policy Directive (PPD)-28[102] with respect to non-U.S. persons in the reauthorization of the Foreign Intelligence Surveillance Act (FISA) (P.L. 112-238).

General Data Protection Regulation (GDPR)

A new EU General Data Protection Regulation (GDPR) enters into force on May 25, 2018, and will be directly applicable in all EU member states, establishing a single set of rules for data protection throughout the EU.[103] Among its provisions, the GDPR identifies what is a legitimate basis for data processing, sets rules regarding data retention and record keeping, requires some companies to hire Data Protection Officers, and establishes new rights for individuals to increase control over their data. The GDPR will apply to all firms doing business in the EU or firms processing the data of EU data subjects, regardless of the company location. While the EU published the final GDPR on May 4, 2016, less than a month before the implementation deadline, the majority of member states do not have the necessary laws and regulations in place to enact GDPR, creating uncertainty for firms doing business in those markets.

High Cost of EU's GDPR

Companies found in violation of the GDPR, including its data breach notification requirements, may be fined up to 4% of their annual worldwide revenues.

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

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

[101] Department of Commerce, *U.S. Secretary of Commerce Wilbur Ross Welcomes Release of the European Commission's Report on the EU-U.S. Privacy Shield*, October 18, 2017, https://www.commerce.gov/news/press-releases/2017/10/us-secretary-commerce-wilbur-ross-welcomes-release-european-commissions.

[102] POLICY DIRECTIVE/PPD-28, January 17, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[103] European Commission, "Agreement on Commission's EU data protection reform will boost Digital Single Market," Press Release, December 15, 2015.

While the EU has begun to release guidance documents,[104] U.S. industry has voiced concern about the potential high cost of data storage and processing needed for compliance and also about the potentially high penalties that may be imposed for violations. Despite the lack of precise guidance, many companies began to analyze the EU regulation and take steps to implement its requirements. 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.[105] To help comply with GDPR, Facebook issued clarified privacy policies and launched a privacy center tool to allow users to more easily control the data they share about themselves and continues to roll out additional updates and changes in response to GDPR requirements and scandals related to data breaches.[106] It is unclear if all of the changes will be only for users inside the EU and not for all users worldwide.[107] It may prove 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. The Administration,[108] ICANN, and other stakeholders have voiced concern that GDPR will limit legitimate business or cooperation efforts, and cybersecurity research or investigators, and are seeking a carve-out.[109]

Some have speculated that the Privacy Shield may become irrelevant once all U.S. companies handling EU residents' data comply with GDPR requirements, potentially simplifying compliance for companies and lessening the burden on U.S. government resources. Some observers note that the EU GDPR may become the de facto global privacy standard given its broad reach, that the United States does not have a comprehensive data privacy policy, and that some developing countries are looking to emulate the GDPR framework.

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 has three pillars:

1. better online access to digital goods and services through cross-border online activity;
2. high-speed, secure, trustworthy infrastructure and a regulatory environment supporting investment and fair competition; and
3. ensuring the digital economy as a driver for growth through investment in infrastructure, research and innovation, and an inclusive society and skilled citizen.

The European Commission's strategy for a digital single market encompasses issues such as the portability of legally acquired content, cross-border data flows within the EU, copyright

[104] European Commission, "Commission publishes guidance on upcoming new data protection rules," January 24, 2018, http://europa.eu/rapid/press-release_IP-18-386_en.htm.

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

[106] Harper Neidig, "Tech giants brace for sweeping EU privacy law," *The Hill*, April 1, 2018.

[107] Mark Scott and Nancy Scola, "Facebook won't extend EU privacy rights globally, no matter what Zuckerberg says," *Politico Pro*, April 19, 2018.

[108] Chris Bing, "White House pushing for research carveout in GDPR," *Cyberscoop*, March 21, 2018.

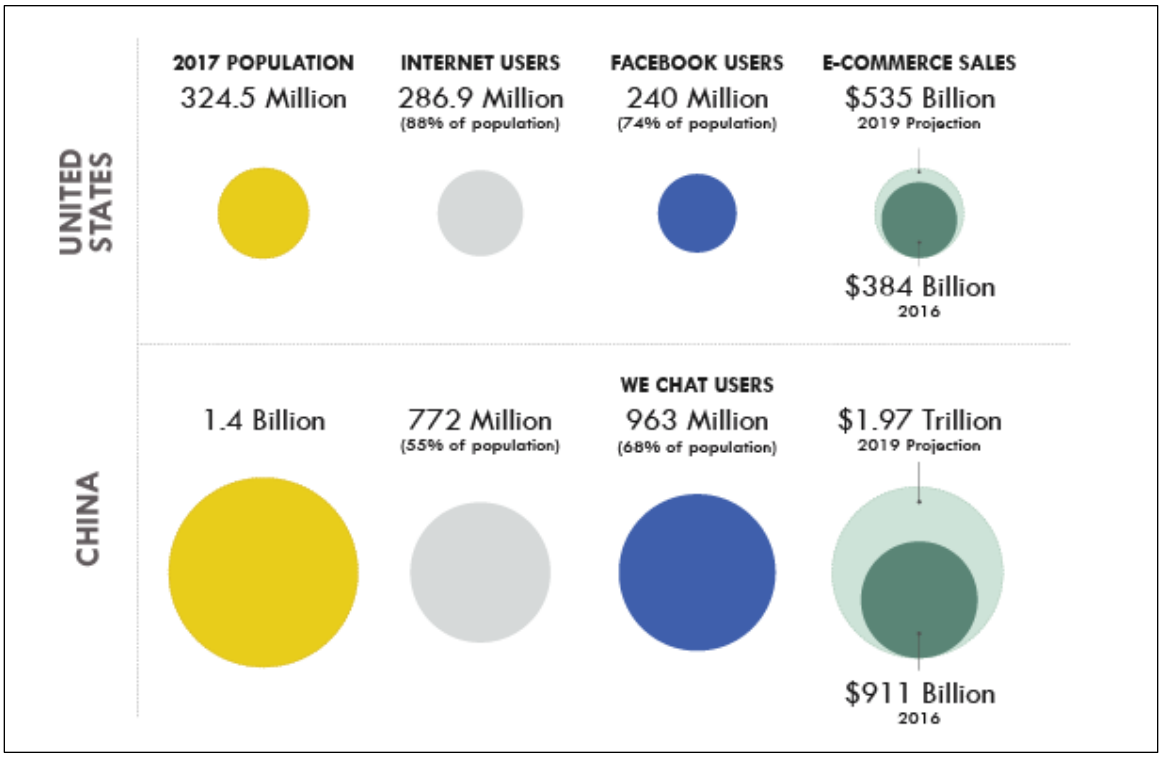
[109] Ivana Janû, ICANN, RE: Request for Guidance: General Data Protection Regulation (GDPR) Impact on the Domain Name System and WHOIS, March 26, 2018, https://www.icann.org/en/system/files/correspondence/marby-to-janu-26mar18-en.pdf.

protection exceptions and limitations, intermediary liability, and enforcement. Some voice concern about the extent to which the finalized DSM regulations will be consistent with U.S. companies' interests. For example, a proposed update of the Audiovisual Media Services Directive (AVMSD) would impose a 30% minimum threshold for European content for internet-based video on-demand providers.[110]

China

With a fundamentally distinct approach to the internet compared to Western countries, China presents a number of significant opportunities and challenges for the United States in digital trade. The Chinese population is more than four times the size of the U.S. population, and China has over two and a half times the number of internet users (see **Figure 7**). U.S. firms may benefit from expanding digital trade in China, but they may also face numerous challenges in the Chinese market.

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



Source: United Nations, Department of Economic and Social Affairs, Population Division (2017). World Population Prospects: The 2017 Revision, DVD Edition. Online sources: Tencent; China Internet Watch; Internetworldstats.com.

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

[110] United States Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*, 2018, p. 185, https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

regulate and control the internet, a concept it has termed "Internet Sovereignty."[111] 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.[112]

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."[113]

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. In 2010, Reuters reported that the USTR considered bringing a WTO dispute settlement case against China's internet censorship of Google and other U.S. internet providers in China.[114] A Google White Paper issued in 2010 stated the following:

> Limitations on the free flow of information and restrictive Internet regulations are a clear threat to open markets and trade. Governments that limit or block the flow of information threaten not only the ability of companies to access and compete in their markets, but also threaten the very traits of the Internet that have made it into an engine of economic growth and put at risk the ability of the Internet-related business to continue expanding their exports, employment, and innovation.[115]

A 2016 report by the USTR cited a number of internet-related barriers. Outright blocking of websites appears to have worsened over the past year, with 8 of the top 25 most trafficked global sites now blocked in China. Examples of blocked sites include Google services (e.g., Gmail), Twitter, Facebook, YouTube, and *The New York Times*. An example of the unpredictability of

---

[111] 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.

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

[113] 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.

[114] Reuters, "U.S. weighing China Internet censorship case: USTR," March 9, 2010, available at https://www.reuters.com/article/us-usa-china-google-wto/u-s-weighing-china-internet-censorship-case-ustr-idUSTRE6284YG20100309.

[115] Google, *Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information*, 2010, p.8, available at https://static.googleusercontent.com/media/www.google.com/en//googleblogs/pdfs/trade_free_flow_of_information.pdf.

China's internet market occurred in April 2016, when Chinese regulators, for unexplained reasons, suspended Apple iTunes Movies and iBooks Store, and DisneyLife services that had been operating in China for months. In its recent FTAs, the United States has attempted to set new digital trade rules to eliminate these types of discriminatory practices and market access barriers.

IP Theft

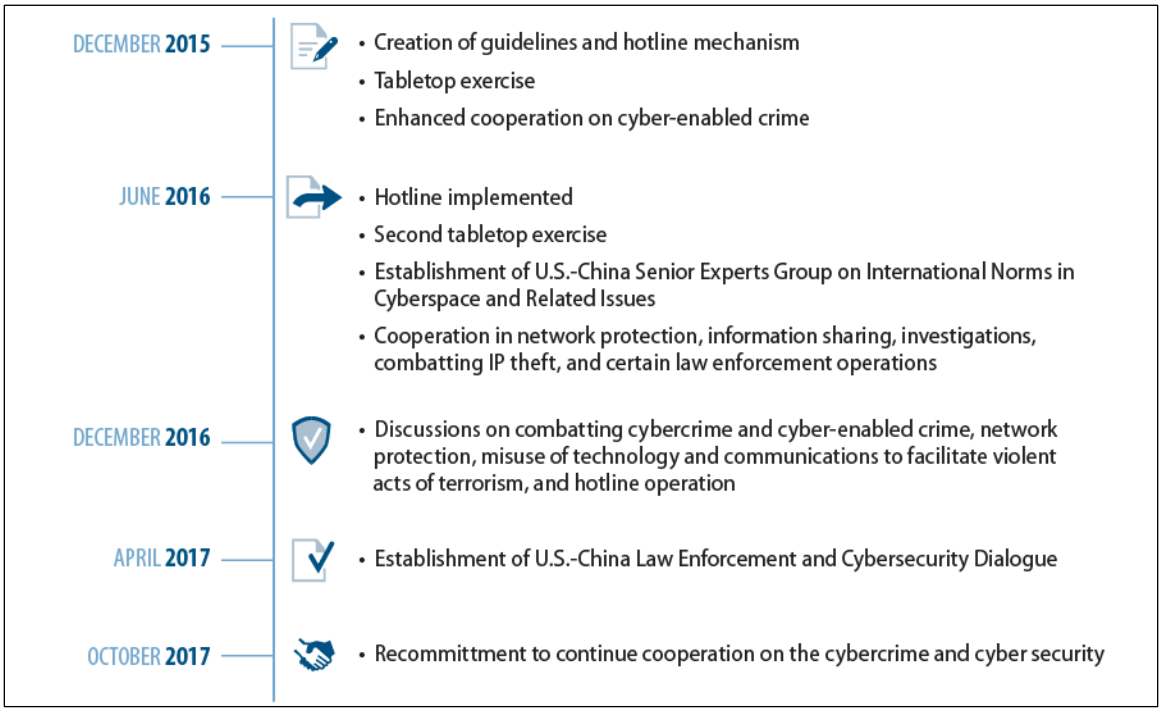
China is considered by most analysts to be the largest source of global theft of IP and a major source of cybertheft of U.S. trade secrets, including by government entities. A 2017 survey by the U.S.-China Business Council found that 94% of respondents said they were concerned about IPR in China. Major IPR issues of concern include restrictions on cross-border data flows in Chinese regulations (65%); inability to utilize global IT solutions or non-Chinese cloud-based applications in China (55%); consumer or company data theft (53%); internet service within China (speed, performance, and accessibility of non-Chinese websites); and IP theft (51%).[116]

In September 2015, the U.S. and Chinese governments reached a framework agreement on economic relations and technology, including IPR.[117] Among the commitments, the parties agreed that regulations should be consistent with WTO commitments and that "neither country's government will conduct or knowingly support cyber-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." Per the agreement, the parties established the U.S.-China High-Level Joint Dialogues on Cybercrime and Related Issues that has met regularly (see **Figure 8**). The effectiveness of the pledge and the ongoing dialogue is subject to debate.

[116] U.S.-China Business Council, *2017 Member Survey*, p. 10, available at https://www.uschina.org/sites/default/files/2017_uscbc_member_survey.pdf.

[117] White House, "FACT SHEET: U.S.-China Economic Relations," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-us-china-economic-relations.

Figure 8. U.S.-China High-Level Joint Dialogues on Cybercrime and Related Issues



Source: CRS based on Department of Homeland Security news releases.

Separate from the bilateral dialogues, 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. However, 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."[118] 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 appear to lay out policies that would require ICT foreign firms to hand over proprietary information. According to the U.S. Department of Commerce:

> The policies set forth in these measures could cause long-term damage to U.S. businesses trying to sell ICT products into China, a market estimated to be worth about $465 billion this year. They also could add significant costs to foreign ICT companies operating in China and could prevent them from supplying the China market with the most technologically advanced and reliable products.[119]

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

[119] U.S. Department of Commerce, *U.S. Fact Sheet: 26th U.S.-China Joint Commission on Commerce and Trade*, November 23, 2016, https://www.commerce.gov/news/fact-sheets/2015/11/us-fact-sheet-26th-us-china-joint-commission-commerce-and-trade.

In December 2016, the Chinese government issued a National Cybersecurity Strategy, which emphasized China's view of cybersovereignty and its right to promulgate policies in line with its own priorities and that no other country should interfere in its cyberspace.[120]

Examples of recently passed or proposed 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;[121] 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.[122]

  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."[123]

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 $12.8 billion in 2015.[124] A U.S. Chamber of Commerce report contends that a decision by China to "purge foreign ICTs" would reduce China's annual GDP by 1.77%, or at least $200 billion (based on 2015 GDP), and would cost the economy at a minimum nearly $3 trillion overall by 2025.[125]

On August 14, 2017, President Trump issued a Presidential Memorandum directing the USTR to determine whether it should launch a Section 301 investigation into China's IPR policies and forced technology transfer polices to determine their impact on U.S. economic interests.[126] On

[120] China Copyright and Media, National Cyberspace Security Strategy, December 27, 2016, available at https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

[121] 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."

[122] 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.

[123] 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.

[124] China was the fourth largest U.S. export market for such services for countries where data is available. See, BEA, *International Trade Data, U.S. Trade in Services*, http://www.bea.gov/iTable/iTable.cfm?ReqID=62&step=1#reqid=62&step=1&isuri=1&6210=4.

[125] U.S. Chamber of Commerce, *Preventing Deglobalization*, March 17, 2016, p. 8, https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf.

[126] 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

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

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 a 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); and (3) propose new investment restrictions on Chinese efforts to acquire sensitive U.S. technology.[127] For example, Chinese acquisitions of U.S. semiconductor companies have come under scrutiny by the Administration and Congress recently.[128] China and the United States initiated a discussion on these trade and other trade concerns in May 2018.[129]

Digital Trade Provisions in Trade Agreements

As the above analysis of EU and China policies demonstrates, there is not a single set international of 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 the 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.

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.

[127] 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.

[128] Reuters, "Chips down: China aims to boost semiconductors as trade war looms," CNBC, April 20, 2018.

[129] The White House, "Statement from the Press Secretary Regarding the United States Delegation to China," April 30, 2018.

WTO Provisions

While no comprehensive agreement on digital trade exists in the WTO, other WTO agreements cover some aspects of digital trade.

General Agreement on Trade in Services (GATS)

The WTO General Agreement on Trade in Services (GATS) entered into force in January 1995, predating the current reach of the internet and 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.[130]

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. Addressing new topics like e-commerce and data flows has been raised but not yet formalized in the WTO.

The 11th WTO Ministerial Conference in Buenos Aires, Argentina, in December 2017 concluded with no clear path forward for comprehensive multilateral negotiations, reflecting an ongoing wide division among members. Advanced economies have pushed for change in the negotiating dynamics, arguing that the WTO needs to address new issues, such as digital trade and investment, especially given the growth of major emerging markets.

On the sidelines of the ministerial, a group of over 70 WTO members, including the United States, agreed to "initiate exploratory work together toward future WTO negotiations on trade related aspects of electronic commerce."[131] USTR supported the movement toward plurilateral efforts stating, "the United States is pleased to work with willing Members on e-commerce, scientific standards for agricultural products, and the challenges of unfair trade practices that distort world markets."[132] Members are currently discussing which aspects of digital trade they will address in any negotiations. The United States put forth its objectives, including market access, data flows, fair treatment of digital products, protection of intellectual property and digital security measures, and intermediary liability, among others.[133]

Declaration on Global Electronic Commerce

In May 1998, WTO members established the "comprehensive" Work Programme on Electronic Commerce "to examine all trade-related issues relating to global electronic commerce, taking into account the economic, financial, and development needs of developing countries."[134] The 1998

[130] 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.

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

[132] U.S. Trade Representative, *USTR Robert Lighthizer Statement on the Conclusion of the WTO Ministerial Conference*, December 2017, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/december/ustr-robert-lighthizer-statement.

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

[134] "Exclusively for the purposes of the work programme, and without prejudice to its outcome, the term 'electronic

declaration establishing the program also included a statement that "members will continue their current practice of not imposing customs duties on electronic transmission."[135]

With the stalling of broader WTO negotiations, multiple members submitted proposals under the existing WTO Work Programme on Electronic Commerce to advance multilateral digital trade negotiations. The U.S. proposal under the Obama Administration reflected and built on the provisions included in the Trans-Pacific Partnership (see below), such as prohibiting digital customs duties and enabling cross-border data flows. China put forward a proposal in which it seeks "to clarify and to improve the application of existing multilateral trading rules" with a focus on facilitating e-commerce.[136] The EU stated that the WTO should focus on consumer protection, nondiscrimination and market access online, trade facilitation, and transparency. India's proposal was the most narrow, suggesting that the WTO focus on the original work program. During the 2017 ministerial meeting, members reached consensus only on extending the customs duties moratorium and continuing on the existing workplan.[137]

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 during the WTO's Tenth Ministerial Conference in December 2015, entering into force 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.

The expanded ITA eliminates tariffs on 201 additional IT products valued at over $1.3 trillion per year.[138] The increased coverage includes, for example, many consumer electronics, new generation semiconductors (multicomponent semiconductors, or MCOs), and medical instruments like magnetic resonance imaging (MRI). According to the USTR, the agreement will provide duty-free access to $180 billion in annual U.S. exports.[139] The parties also agreed to review the agreement's scope no later than 2018 to determine if additional product coverage is warranted as technology evolves, and have also begun to look at nontariff barriers.

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.

---

commerce' is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means." For more information, see https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

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

[136] WTO, "Communication from the People's Republic of China," JOB/CTG/2, November 4, 2016.

[137] WTO Work Programme on Electronic Commerce, "Draft Ministerial Decision," December 13, 2017.

[138] World Trade Organization, *WTO members conclude landmark $1.3 trillion IT trade deal*, December 16, 2015, https://www.wto.org/english/news_e/news15_e/ita_16dec15_e.htm.

[139] Office of the U.S. Trade Representative, *U.S. and WTO Partners Announce Final Agreement on Landmark Expansion of Information Technology Agreement*, December 2015, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/december/US-WTO-Partners-Announce-Final-Agreement-on-Expansion-ITA.

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 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.[140]

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.[141]

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.[142]

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

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

[141] 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.

[142] WTO, General Council, "Item 6—Work Programme on Electronic Commerce—Review of Progress," WT/GC/W/701, July 24, 2015.

create new online rights, and to maintain a fair balance between the owners of rights and the general public.[143]

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.[144]

As of December 2017, 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.[145] 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."[146] The United States has continued to call on trading partners, such as Turkey and Mexico, to fully implement the WIPO Internet Treaties.[147]

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 stalled multilateral negotiations and the desire by some parties to address new topics such as e-commerce are two of the drivers behind the growth of bilateral and plurilateral trade agreements inside and outside of the WTO. 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.[148] 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.[149] Most chapters contain provisions on nondiscrimination of digital products, prohibition of customs duties, transparency, and cooperation topics such as

---

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

[144] 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.

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

[146] 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.

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

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

[149] 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.

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.[150] 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 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."[151]

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

Trans-Pacific Partnership (TPP) Agreement

On January 24, 2017, President Trump withdrew the United States from the Trans-Pacific Partnership (TPP). The TPP was a proposed FTA among 12 countries in the Asia-Pacific region, including the United States. The 11 remaining TPP countries concluded a revised Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP or TPP-11) based on the TPP and planned to come into force without the United States that kept intact the digital-trade related provisions (but excluded select IPR commitments).[152]

The TPP-11 includes commitments to address barriers to digital trade beyond the provisions in KORUS and earlier U.S. FTAs. Overall, the agreement aims to promote digital trade, promote the free flow of information, and ensure an open internet. Provisions related to digital trade are included in multiple chapters (e.g., e-commerce, financial services, telecommunications, intellectual property rights), showing the complexity of digital trade barriers and issues. The CPTPP encourages parties to become members of the tariff-eliminating WTO Information Technology Agreement.

The TPP-11 has several digital trade-related innovations for trade agreements, including the following:

- Prohibits cross-border data flow restrictions and data localization requirements, except for financial services and government procurement.

[150] 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.

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

[152] Chieko Tsuneoka, " TPP Members Reach Agreement on Major Trade Pact," Wall Street Journal, January 23, 2018.

- Prohibits requirements for source code disclosure or transfer as a condition for market access, with exceptions.
- Requires parties to have online consumer protection and antispam laws, and a legal framework on privacy.
- Prohibits requiring technology transfer or access to proprietary information for products using cryptography.
- Clarifies IPR enforcement rules to provide criminal penalties for trade secret cybertheft.
- Encourages cooperation between parties on e-commerce to assist SMEs, and on privacy and consumer protection.
- Promotes cooperation on cybersecurity.
- Safeguards cross-border electronic card payment services.
- Covers mobile service providers and promotes cooperation for international roaming charges.

The agreement requires parties to have a legal framework to protect personal information. Critics contend that the provisions are vague and do not contain an explicit minimum standard for privacy protection. Supporters note the reference to take into account "guidelines of relevant international bodies" that may include the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[153]

North American Free Trade Agreement (NAFTA)

Like the WTO agreements, NAFTA predated mass usage of the internet, having entered into force on January 1, 1994.[154] In May 2017, the Trump Administration notified Congress of its intent to begin talks with Canada and Mexico to renegotiate and modernize NAFTA, providing an opportunity to address digital trade.[155] USTR's updated negotiating objectives are similar to TPP (see above) and include language for mandating nondiscriminatory treatment of digital products transmitted electronically; prohibiting restrictions on cross-border data flows or imposition of localization requirements for servers; preventing mandated disclosure of source code or algorithms; proscribing customs duties for digital products delivered electronically; and preventing or eliminating government involvement in cybertheft of intellectual property.[156]

As all NAFTA parties were involved in the TPP negotiations and Mexico and Canada are members of the TPP-11, some have suggested the TPP text could provide a starting point. Some stakeholders contend that a revised NAFTA should go beyond the TPP provisions, such as setting a *de minimis* threshold equal to that in U.S. law to encourage e-commerce exports by U.S. small and mid-size businesses.[157] Others have advocated that NAFTA require that each party have a cybersecurity legal framework. NAFTA negotiations are ongoing.

---

[153] TPP Chapter 14, Article 14.8.2.

[154] For more information on NAFTA, please see CRS Report R42965, *The North American Free Trade Agreement (NAFTA)*, by M. Angeles Villarreal and Ian F. Fergusson.

[155] For more information on the notification and Trade Promotion Authority requirements please see, CRS In Focus IF10038, *Trade Promotion Authority (TPA)*, by Ian F. Fergusson.

[156] Office of the United States Trade Representative, *Summary of Objectives for the NAFTA Renegotiation*, November 2017, https://ustr.gov/sites/default/files/files/Press/Releases/Nov%20Objectives%20Update.pdf.

[157] *De minimis* is threshold for assessing customs duties on imported goods.

Trade in Services Agreement (TiSA) Negotiations

Negotiations on a proposed plurilateral Trade in Services Agreement (TiSA) were launched in April 2013, and are occurring outside of the WTO.[158] The 23 TiSA participants account for about 70% of world trade in services and include the United States, EU, and Australia. Some key major emerging markets, including Brazil, China, and India, are not currently parties to the TiSA negotiations.

Though the final structure and sectors to be covered in TiSA remain under negotiation, setting common rules for digital trade is a key interest of the United States. The chapter or annex on digital trade or e-commerce would likely address trade barriers to cross-border data flows, consumer online protection, and interoperability, among other areas, similar to the provisions in the proposed TPP.[159] Two obstacles in TiSA negotiations, however, have been the EU's reluctance to put forward a proposal on data flows or to commit to including "new services" (many of which are likely to be digital) under TiSA nondiscrimination obligations.[160]

Requiring regulatory cooperation and ongoing dialogue on digital trade issues between TiSA members could provide a path forward without changing existing laws in each TiSA country. Negotiators could decide to include international regulatory cooperation on matters of cybersecurity or in support of small and mid-sized enterprises as in TPP. Negotiators may aim for language that is open enough to enable nondiscriminatory and open trade and address evolving technology, but concrete enough for regulators to protect privacy and safeguard cybersecurity.

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 may be 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.

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.[161] At the 2017 meeting, the G-20 leaders issued a communique with a commitment to "ensure effective competition" including openness, transparency, international standards, and interoperability. They also recognized the importance of consumer protection, IPR, privacy, and security.

---

[158] For more on TiSA, see CRS In Focus IF10311, *Trade in Services Agreement (TiSA) Negotiations*, by Rachel F. Fefer, and CRS Report R44354, *Trade in Services Agreement (TiSA) Negotiations: Overview and Issues for Congress*, by Rachel F. Fefer.

[159] *Inside U.S. Trade*, "Despite 'TISA-Plus' Aims, EU's E-Commerce Proposal For T-TIP Falls Short," August 13, 2015.

[160] Washington Trade Daily, November 10, 2016.

[161] 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.

OECD. The OECD offers yet another forum to discuss principles and norms to facilitate a thriving digital economy. The June 2016 Ministerial Meeting in Mexico, titled "Digital Economy: Innovation, Growth and Social Prosperity," addressed an open internet and data flows; infrastructure and connectivity; digital trust; and workforce skills.[162] The Ministerial Declaration included recognizing the growth and transforming impact of the digital economy as well as evolving challenges, and declared support of the free flow of information, innovation and emerging technologies, and the need to build trust, reduce impediments to e-commerce, and enable opportunities.[163] The declaration also acknowledged the need to balance public policy objectives and incorporate a whole-of-society perspective. The United States could work with OECD partners to reinforce these principles by defining specific action plans or commitments.

The OECD issued a series of reports in 2017 related to digital trade including an assessment of the digital transformation of each OECD economy.[164] The report identified specific challenges and recommendations, including establishing a national digital strategy.

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.[165] The APEC Electronic Commerce Steering Group (ECSG) coordinates e-commerce activities for APEC and promotes the development and use of e-commerce legal, regulatory, and policy environments that are predictable, transparent, and consistent. Within the ECSG, APEC is implementing a Cross-Border Privacy Rules (CBPR) system to be consistent with the already established APEC Privacy Framework.[166] According to BSA, 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.[167] Currently, the United States, Canada, Mexico, South Korea, Japan, and Singapore are full participants in the CBPR system, while Taiwan and Philippines have announced plans to participate. 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.

While APEC initiatives are regionally focused, because they reflect economies at different stages of development and include industry participation, they can provide a basis to scale up to larger global efforts. Due to its voluntary nature, APEC can serve 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,

[162] http://www.oecd.org/internet/ministerial/. The G-7 is a subset of the G-20 and includes Canada, France, Germany, Italy, Japan, United Kingdom, and the United States.

[163] OECD Ministerial Declaration, May 2016, http://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf.

[164] 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.

[165] 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.

[166] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx.

[167] 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 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 potential legislative and oversight implications. Issues include the following.

- 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.
- 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.
- Effectively addressing important digital trade barriers and cybertheft.
- Considering if the United States would benefit from overarching digital privacy policy and what lessons can be drawn from other countries' experiences.
- Examining how best to balance market openness with other policy goals such as right to privacy and the government's need for access to protect safety and national security.
- 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 NAFTA and WTO plurilateral efforts in addressing U.S. trade barrier concerns, and setting new rules and disciplines, as well as potential standard-setting practices that may have global reach, including by the EU and China.
- Assessing the effectiveness of the U.S.-China bilateral cyber dialogue, including review of the Trump Administration's Section 301 actions and other bilateral efforts.

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

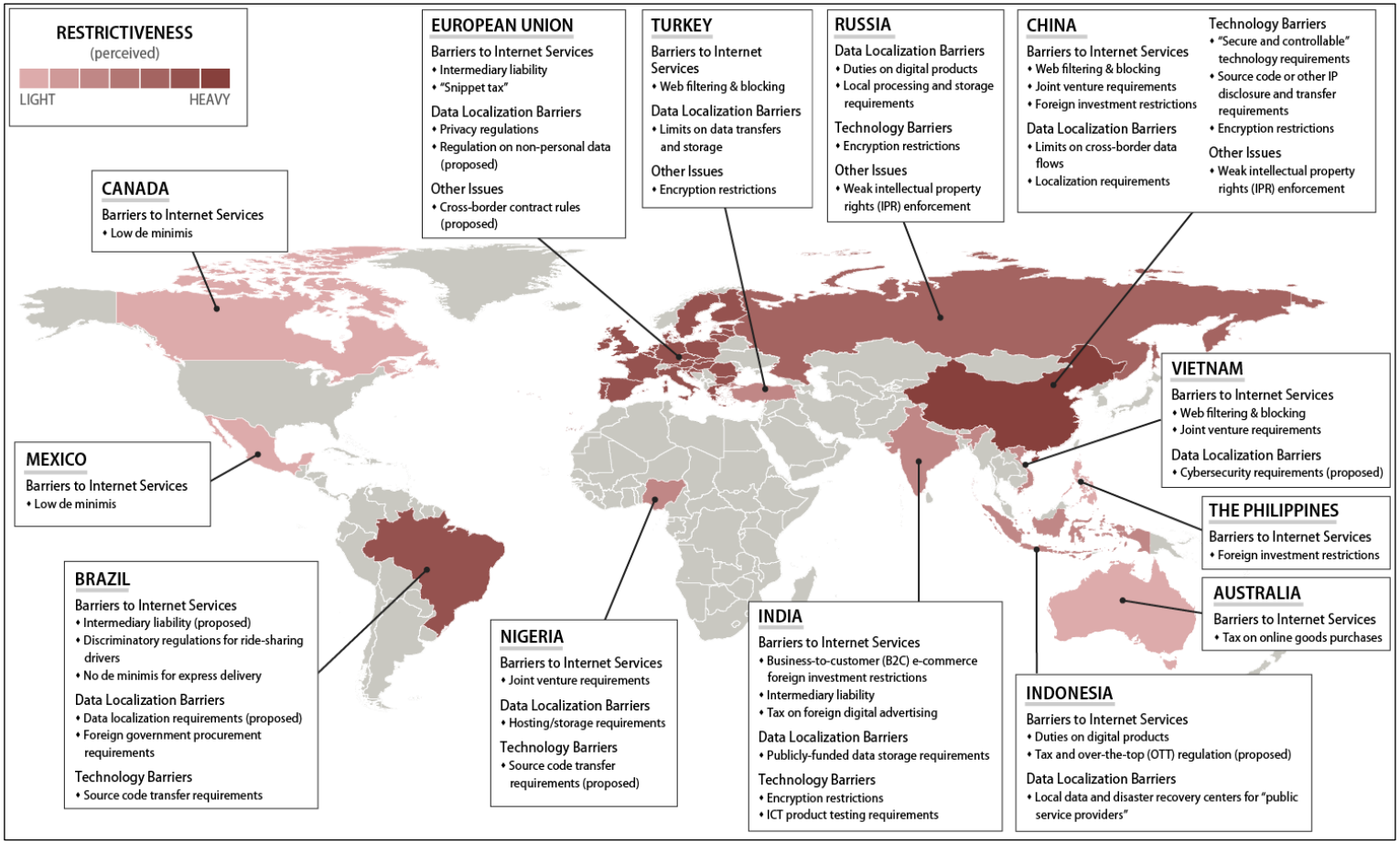
- Restrictions or prohibitions on use of encryption
- Source code, technology, or other intellectual property rights (IPR) forced transfer requirements
- Local testing and certification for imported information technology (IT) equipment may add costs or delays for imported goods

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.