

Digital Trade and U.S. Trade Policy

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

Shayerah Ilias Akhtar
Specialist in International Trade and Finance

Wayne M. Morrison
Specialist in Asian Trade and Finance

June 6, 2017

Congressional Research Service
7-5700
www.crs.gov
R44565

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

As the rules of global Internet develop and evolve, digital trade has risen in prominence on the global trade and economic agenda, but multilateral trade agreements have not kept pace with the complexities of the digital economy. 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. According to one source, the volume of global data flows grew 45-fold from 2005 to 2014, faster than international trade or financial flows. 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 to implement new trade rules and disciplines through ongoing trade negotiations, and also working 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 like movies and video games and services such as email. Digital trade also enhances the productivity and overall competitiveness of an economy. According to the U.S. International Trade Commission, U.S. domestic and international digital trade added 3.4%-4.8% ($517.1-$710.7 billion) to the U.S. gross domestic product (GDP) in 2011. The Department of Commerce found that in 2014, digitally delivered services accounted for more than half of U.S. services trade.

The increase in digital trade also 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, unique standards or burdensome testing, filtering or blocking, and cybercrime exposure or state-directed theft of trade secrets.

Digital trade issues often overlap and cut across policy areas, including IPR and national security; this raises questions for Congress as it weighs different policy objectives. The Organization for Economic Cooperation 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 comprehensive agreement on digital trade exists in the World Trade Organization (WTO), other WTO agreements do 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 potential Trans-Pacific Partnership (TPP), Transatlantic Trade and Investment Partnership (T-TIP), and plurilateral Trade in Services Agreement (TiSA) are expected to address digital trade to varying degrees. Digital trade norms are also being discussed in forums such as the Group of 20 (G-20), the OECD, and the Asia-Pacific Economic Cooperation (APEC), providing the United States with multiple opportunities to engage in and shape global developments.

With workers in the high-tech sector in every U.S. state and congressional district, Congress has an interest in ensuring the global rules and norms of the Internet economy are 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
Digitization of Trade Flows 5
Economic Impact of Digital Trade 6
Digitization Challenges 7
Digital Trade Barriers and Policy Issues 10
Tariff Barriers 11
Nontariff Barriers 13
Localization Requirements 13
Intellectual Property Rights (IPR) Infringement 15
National Standards and Burdensome Conformity Assessment 18
Filtering, Blocking, and Net Neutrality 18
Cybersecurity Risks 19
U.S. Digital Trade with the EU and China 20
European Union 20
China 22
Internet Governance 22
IP Theft 23
New Restrictions on Information and Communications Technology 23
U.S.-China BIT Negotiations 26
Digital Trade Provisions in Trade Agreements 28
WTO Provisions 28
General Agreement on Trade in Services (GATS) 28
Information Technology Agreement (WTO ITA) 29
Declaration on Global Electronic Commerce 29
Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) 30
World Intellectual Property Organization (WIPO) Internet Treaties 31
Future Sectoral Approaches 32
U.S. Bilateral and Plurilateral Agreements 32
Existing U.S. Free Trade Agreements (FTAs) 33
The Proposed Trans-Pacific Partnership (TPP) Agreement 33
Trade in Services Agreement (TiSA) Negotiations 35
Transatlantic Trade and Investment Partnership (T-TIP) Negotiations 36
Other International Forums for Digital Trade 36
Policy Issues for Congress 38

Figures

Figure 1. Growth in Global Data Flows 2
Figure 2. A Typical Day in the Life of the Internet 3
Figure 3. Data and Communication Flows between Regions 4
Figure 4. What is Digital Trade? 9

Contacts

Author Contact Information 39
Acknowledgments 39

Introduction

The Internet-driven digital revolution is causing fundamental change to the global economy leading not only to new modes of communication and information-sharing, new business models, and new sources of job growth, but also to new policy questions and concerns. According to a report by the McKinsey Global Institute, globalization has entered "a new era defined by data flows that transmit information, ideas, and innovation."[1] Another report noted "information is currency.... Information is also the building block of the digital economy."[2] As digital information increases in importance in the U.S. economy, issues related to digital trade have become of growing interest in trade negotiations.

The U.S. International Trade Commission (ITC) broadly defines digital trade as "U.S. domestic commerce and international trade in which the Internet and Internet-based technologies play a particularly significant role in ordering, producing, or delivering products and services."[3] Thus, digital trade not only includes end-products like movies and video games, but also provides the means to enhance the productivity and overall competitiveness of an economy. Examples of digital trade include orders placed on an e-commerce website; information streams needed by manufacturers to manage global value chains; communication channels such as email and voice over Internet protocol (VoIP); and financial data and transactions relied on for online purchases or electronic banking.

The rules governing digital trade are evolving as governments across the globe experiment with different approaches and try to balance diverse policy priorities and objectives. Barriers to digital trade, such as infringement of intellectual property rights (IPR), national security measures, or industrial policies, often overlap and cut across sectors. Digital trade issues have been in the spotlight recently, due in part to heightened concerns over data privacy and an increasing number of cybertheft incidents that have affected U.S. consumers and companies. These concerns may affect the general U.S. interest in promoting cross-border data flows. 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 digital issues in trade agreements, including the proposed Trans-Pacific Partnership (TPP), which contains the most advanced disciplines to date on digital trade barriers. Congress has an important role in shaping digital trade policy, from oversight of agencies charged with regulating cross-border data flows and of ongoing trade negotiations, to working with the executive branch to identify the right balance between digital trade and other policy objectives, including privacy and national security concerns.

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] James Manyika, et al., *Digital globalization: The new era of global flows*, February 2016, http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows?cid=other-eml-alt-mgi-mck-oth-1602.

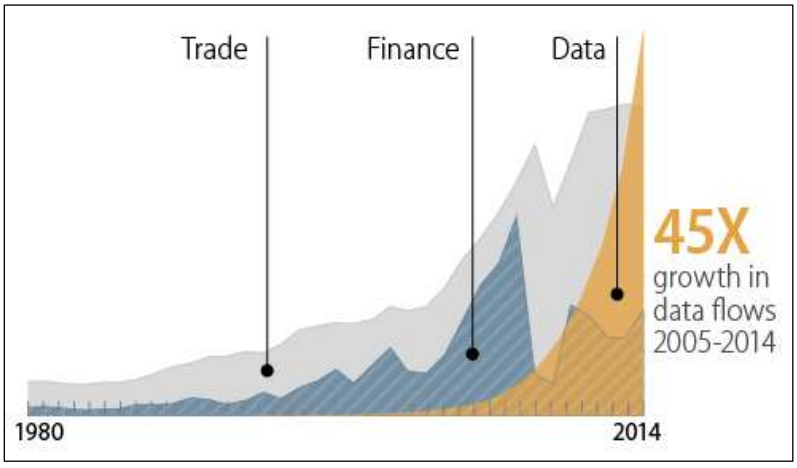
[2] Susan Ariel Aaronson, *The Digital Trade Imbalance and Its Implications for Internet Governance*, Centre for International Governance Innovation and Chatham House, 2016, p. 1, https://www.cigionline.org/sites/default/files/gcig_no25_web_0.pdf.

[3] U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, Publication No: 4485, Investigation No: 332-540, p.29, August 2014, https://www.usitc.gov/publications/332/pub4485.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 a study by the Boston Consulting Group, the global economic impact of the Internet is estimated to be $4.2 trillion in 2016, and would rank as the fifth-largest national economy in the world. Some estimates indicate that gross domestic product (GDP) in developed countries is 5% to 9% higher annually (largely through increased productivity and lower costs) than it would be without the Internet, while in developing countries the Internet has an even larger impact, adding 15% to 25% to GDP per year.[4] According to one estimate, the volume of global data flows is growing faster than trade or financial flows, as **Figure 1** illustrates, growing 45-fold from 2005 to 2014.

Figure 1. Growth in Global 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. Today, there are more than 2.7 billion Internet users worldwide.[5] World Bank estimates are even higher, showing that Internet users tripled since 2005 to 3.2 billion in 2015, representing 60% of people globally.[6] The Organization for Economic Cooperation 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.[7] In the United States, 92% of the population uses the Internet, according to

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

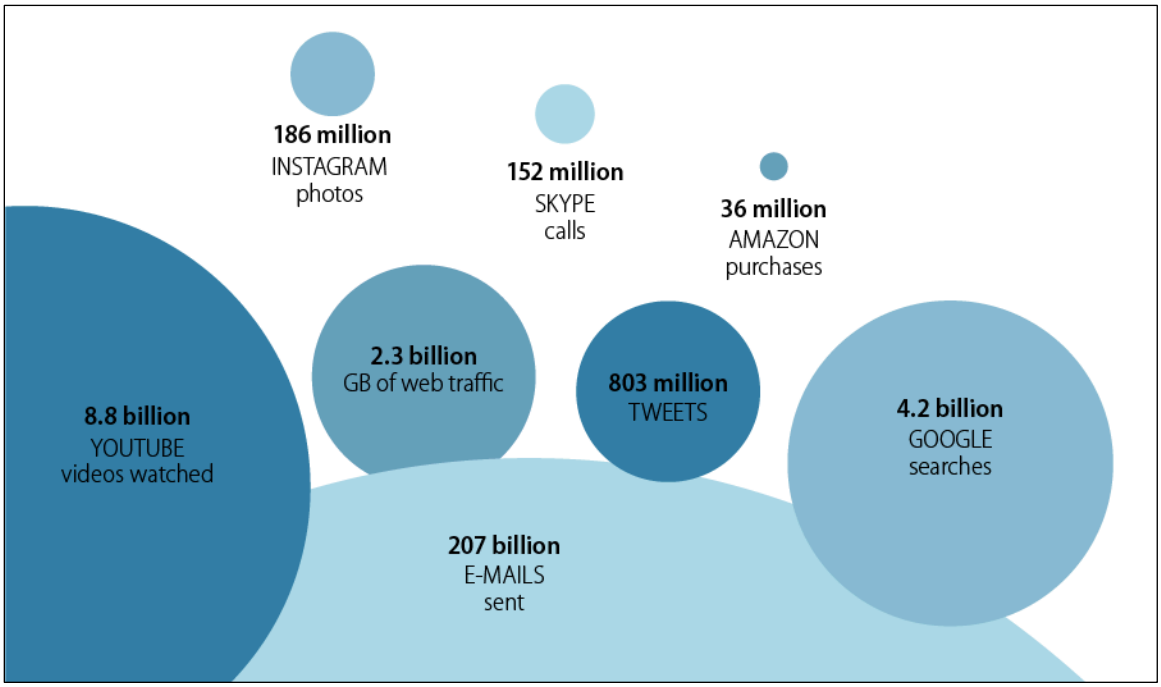
[5] Business Software Alliance, *Powering the Digital Economy: A Trade Agenda to Drive Growth*, 2015, http://www.bsa.org/~/media/Files/Policy/Trade/DTA_study_en.pdf.

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

[7] 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.

one estimate.[8] While 75% of U.S. households use wired Internet access, an increasing number (20%) are relying on mobile Internet access, with low-income households more likely to rely on wireless (29%). While the percentage of American consumers relying on a desktop or laptop at home is declining (34% and 46%, respectively), they increasingly are turning to an array of devices from smartphones to wearable devices for Internet access, according to one estimate.[9] Each day, companies and individuals depend on the Internet to communicate and transmit data via various media and channels that continue to expand (see **Figure 2**).

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.

According to one study, global cross-border Internet traffic grew 60% a year between 2002 and 2012.[10] Some analysts also conclude that most of the bilateral trade in data-intensive sectors takes place between countries in the OECD, and find a correlation with foreign direct investment (FDI).[11] OECD countries are also more likely to have the necessary underlying infrastructure to support high data flows.

[8] 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.

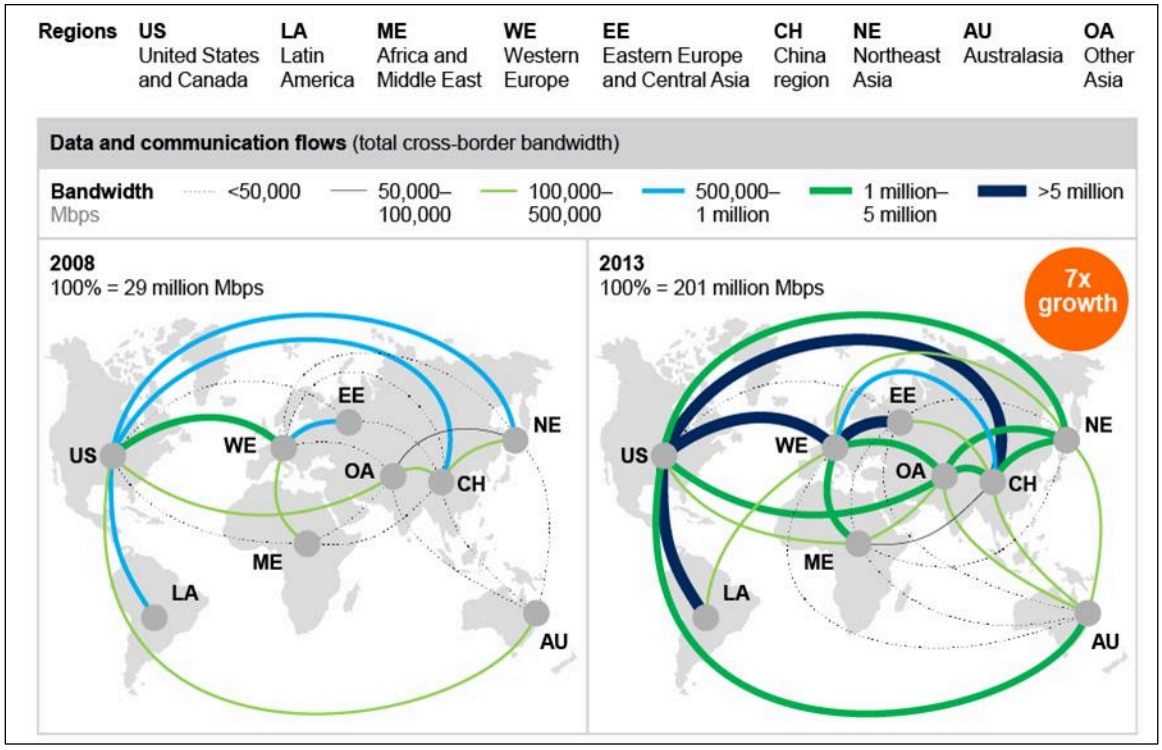
[9] Giulia McHenry, *Evolving Technologies Change the Nature of Internet Use*, National Telecommunications & Information Administration blog, April 19, 2016.

[10] Susan Lund and James Manyika, *Strengthening the Global Trade and Investment System for Sustainable Development: How Digital Trade is Transforming Globalization*, The E15 Initiative. McKinsey & Company., January 2016, http://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation/.

[11] Erik van der Marel, *Disentangling the Flows of Data: Inside or Outside the Multinational Company?*, European Center for International Political Economy, July 2015, http://ecipe.org/publications/flows-data-inside-outside-multinational-company/?chapter=all.

Cross-border data and communication flows are themselves 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. According to one estimate, worldwide data and communication flows have grown more than sevenfold from 2008 to 2013 (See **Figure 3**).[12] The highest levels reportedly are those flows between the United States and Western Europe, Latin America, and China.

Figure 3. Data and Communication Flows between Regions



Source: McKinsey Global Institute, *Global Flows in a digital age: How trade, finance, people, and data connect*, April 2014, p. 13, http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age.

Notes: Circle indicates size of increase.

Powering all these connections and data flows are underlying information and communication technologies (ICT).[13] The Business Software Alliance (BSA) estimates that over $2 trillion are spent each year on information technologies and services. ICT spending is a large and growing component of the international economy. Globally, ICT spending is growing at a compounded annual rate of 3.4%, and is forecasted to be more than $4 trillion in 2017. In 2012, the United States was estimated to be the largest purchaser of ICT at $942 billion.[14]

[12] James Manyika, Jacques Bughin, and Susan Lund, et al., *Global Flows in a digital age: How trade, finance, people, and data connect*, McKinsey Global Institute, April 2014, http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age.

[13] 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.

[14] Business Software Alliance, *Powering the Digital Economy: A Trade Agenda to Drive Growth*, January 2014, p.8-9, http://digitaltrade.bsa.org/pdfs/DTA_study_en.pdf.

ICT services are outpacing the growth of international trade in ICT goods. According to the OECD, ICT services increased fourfold between 2001 and 2013. The United States is the fourth-largest OECD exporter of ICT services, after Ireland, India, and Germany.[15] ICT services include telecommunications and computer services as well as related charges for the use of intellectual property (e.g., licenses and rights) while ICT-enabled services are those services with outputs delivered remotely over ICT networks such as online banking or education. According to the U.S. Bureau of Economic Analysis (BEA), in 2015, exports of ICT services accounted for $65 billion of U.S. exports while potentially ICT-enabled services exports were another $399 billion, demonstrating the impact of the Internet and digital revolution.[16]

Digitization of Trade Flows

As the Internet and technology continue to develop, increasing digitization affects finance and data flows, as well as the movement of people and goods. Beyond simple communication, McKinsey describes three major ways digital technologies affect global trade flows:[17]

1. Digitization creates new digital goods and services. Digital technology enables innovation. By transforming, and often replacing, traditional goods and services, or the need for people to travel, new products are conceived (e.g., e-books, remote or virtual office for collaboration, tele-medicine, online education or banking).
2. Digitization enhances physical flows through "digital wrappers." Digital wrappers add value by raising productivity, and/or lowering the costs and barriers related to flows of traditional goods and services (e.g., radio-frequency identification [RFID] tags for supply chain tracking, data files used in 3-D printing [or additive manufacturing], cars automatically transmitting data, the "Internet of Things" to connecting devices or objects).[18]
3. Digitization provides platforms that serve as intermediaries for production, exchange, and consumption.[19] Intermediary platforms include not only those used in e-commerce, but also for social media, crowd funding, cloud computing,

[15] OECD. (2015), "Chapter 2: The foundations of the digital economy," *OECD Digital Economy Outlook 2015*, p. 92, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264232440-2-en.

[16] Alexis N. Grimm, *Trends in U.S. Trade in Information and Communications Technology (ICT) Services and in ICT-Enabled Services,* BEA, May 2016, http://www.bea.gov/scb/pdf/2016/05%20May/0516_trends_%20in_us_trade_in_ict_serivces2.pdf

[17] Susan Lund and James Manyika, *Strengthening the Global Trade and Investment System for Sustainable Development: How Digital Trade is Transforming Globalization*, The E15 Initiative. McKinsey & Company., January 2016, http://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation/.

[18] The OECD defines the Internet of Things as "encompassing all devices and objects whose state can be read or altered via the internet, with or without the active involvement of individual... 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." OECD (2015), *OECD Digital Economy Outlook 2015*, p. 61, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264232440-2-en.

For more information on the Internet of Things, see CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer.

[19] This is distinct from the physical infrastructure platforms for data and connectivity that these digital platforms rely on.

search engines, big data analytics, sharing services (e.g., car or accommodation sharing such as Uber or Airbnb), and mobile "apps," or applications.[20]

Economic Impact of Digital Trade

The World Bank identifies three buckets of "digital dividends," benefits that result from using digital technologies: (1) inclusion through increased access and reach; (2) efficiency through automation and coordination; and (3) innovation driving new businesses.[21] These dividends can accrue to businesses, individuals, and governments. Firms that use the Internet more intensively show higher productivity and tend to be larger, faster-growing, and more skill and export intensive. An increase in Internet usage is also associated with an increase in the number and value of products being traded. Drilling down further into the economic benefits of digital trade, the ITC identified specific benefits for consumers and workers (e.g., reduced prices, increased selection, and higher employment) and businesses (e.g., increased efficiency, productivity, output, exports, and sales).[22]

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.[23]

The Information Technology & Innovation Foundation reports that every U.S. state and congressional district has "... some kind of technology and innovation-driven activity occurring locally, either because long-established industries such as agriculture, mining, manufacturing, and professional services are rapidly evolving into tech-enabled industries, or because new developments such as cloud computing and ubiquitous access to broadband Internet service..."[24]

Looking at digital trade in an international context, global cross-border e-commerce from online sales (excluding domestic sales) was estimated to be 10% to 15% of total e-commerce in 2014.[25] In the same year, the United States exported $399.7 billion in digitally deliverable services, and imported $240.8 billion, creating a surplus of $158.9 billion. Digitally delivered services accounted for more than half of all U.S. services trade, according to the Department of Commerce.[26] Other estimates show that, without the Internet, the costs of U.S. imports and

[20] According to the U.S. National Institute of Standards and Technology, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. For more information, see CRS Report R42887, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, by Patricia Moloney Figliola and Eric A. Fischer.

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

[22] 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. 6-1, https://www.usitc.gov/publications/332/pub4415.pdf.

[23] 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.

[24] 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.

[25] BCG, "Cross Border E-Commerce," September 18, 2014.

[26] Department of Commerce Economics and Statistics Administration, *Digitally Deliverable Services Remain an Important Component of U.S. Trade*, May 28, 2015, http://www.esa.doc.gov/economic-briefings/digitally-deliverable-services-remain-important-component-us-trade.

exports would have been an average of 26% higher.[27] Furthermore, 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.

Digital platforms can minimize costs and enable small and medium-sized enterprises (SMEs) to grow through extended reach or integrating into a global value chain (GVC) (see **text box**). As a result, more firms are able to conduct business in global markets (or are more willing to do so), while the digitization of customs and border control mechanisms helps simplify and speed delivery of goods to customers. A study of U.S. SMEs on the e-commerce platform eBay found that 97% export while that number is a full 100% in countries as diverse as Peru and Ukraine.[28]

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

Idaho Company Thrives with Digital Trade

TSheets co-founders 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 even 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.[30]

Digitization Challenges

The U.S. economy may only be realizing 18% of its digital potential, and it is doing so unevenly across sectors and populations.[31] 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.[32]

Additionally, sources of "e-friction" or obstacles can prevent consumers, companies, and countries from realizing the full benefits of the online economy.[33] Causes of e-friction can fall

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] Ibid.

[33] Paul Zwillenberg, Dominic Field, and David Dean, *Greasing the Wheels of the Internet Economy*, Boston Consulting Group, February 2014.
(continued...)

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.[34]

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 a tendency for some to use the Internet to establish monopolies.[35] While new technologies and new business models present opportunities to enhance efficiency and expand revenues, innovate faster, and achieve other benefits, new challenges also arise with the disruption of supply chains, labor markets, and some industries.

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.[36] 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.[37]

(...continued)

https://www.bcgperspectives.com/content/articles/digital_economy_telecommunications_greasing_wheels_internet_economy/.

[34] Ibid.

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

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

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

Figure 4. What is Digital Trade?

Examples of international digital trade



Source: CRS.

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

Digital Trade Barriers and Policy Issues

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. Ensuring a free and open Internet is a stated policy priority for the U.S. government.[38] Like other cross-cutting policy areas, such as cybersecurity, 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.

Ensuring a Free and Open Internet[39]

Ensuring a free and open Internet is a policy priority according to the U.S. Department of State. The U.S. Trade Representative aims to promote this position through global trade.

"Digital freedom must triumph over digital protectionism. Around the world, policies restricting the free flow of data and the openness of the Internet are on the rise, threatening to effectively balkanize the Internet... Policies requiring companies to store data locally present another serious threat, making costs prohibitively high for many small businesses, curtailing access to global services, and stifling innovation...

Above and beyond its impact on commerce, digital freedom goes to the heart of what it means to live in the information age. Ensuring that the rules of the road for global trade promote the free flow of information and resist artificial barriers has broad ramifications. When data flows are obstructed, everyone from the immigrant keeping in touch with relatives, to the work-from-home entrepreneur connecting with customers, to the aspiring high school blogger can be affected."—U.S. Trade Representative, Ambassador Michael Froman.

The Department of Commerce National Telecommunications and Information Administration notes key U.S. policies that enable a strong digital economy in this country include (1) connecting and empowering users; (2) trusting the private sector and protecting online platforms; (3) a strong and balanced approach to intellectual property that fosters innovation while recognizing "fair use"; and (4) a multi-stakeholder consensus-based process for Internet governance.[40] The absence of similar policies, or the existence of opposing ones, outside the United States can lead to trade barriers that hinder or block the flow of digital trade.

The Department of Commerce launched a Digital Economy Agenda that identifies four pillars:[41]

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;

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

[39] Ambassador Michael B.G. Froman, "Getting Trade Right," *Democracy Journal*, Fall 2015, http://democracyjournal.org/magazine/38/getting-trade-right-1/. For more information, see also: The President of the United States, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[40] John B. Morris Jr., Twenty Years after the Birth of the Modern Internet, U.S. Policies Continue to Help the Internet Grow and Thrive, May 1, 2015, https://www.ntia.doc.gov/blog/2015/twenty-years-after-birth-modern-internet-us-policies-continue-help-internet-grow-and-thriv.

[41] 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.

2. Promoting trust online, because security and privacy are essential if electronic commerce is to flourish;
3. Ensuring access for workers, families, and companies, because fast broadband networks are essential to economic success in the 21st century; and
4. Promoting innovation, through smart intellectual property rules and by advancing the next generation of exciting new technologies.

The Commerce Secretary launched specific efforts to support the Digital Economy Agenda, including a Digital Economy Board of Advisors from across sectors 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.[42]

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. The ITC estimated 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.[43]

2015 U.S. Digital Trade Negotiating Objectives

Congress enhanced its digital trade 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.[44] 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 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

Tariffs may impede goods trade at the border by raising the prices of U.S. products as costs are passed to end customers, thus limiting market access for U.S. exporters. Quotas may limit the number or value of foreign goods, persons, suppliers, or investments allowed in a market.

[42] Secretary of Commerce Penny Pritzker, "Commerce Launches Digital Attaché Program to Address Trade Barriers," March 11, 2016, https://www.commerce.gov/news/opinion-editorials/2016/03/commerce-launches-digital-attache-program-address-trade-barriers.

[43] 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.

[44] 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.

Global exports of ICT goods reached $1.6 trillion in 2013, and production is increasingly concentrated in a few countries, with China (32% of ICT good exports), the United States (9%), and Singapore (8%) ranking at the top.[45] Forecasts for IT spending in 2017 are mixed as analysts weigh the potential impacts of new policies under the Trump Administration and the UK's departure from the EU, among other factors.[46] Semiconductors, a key component in many electronic devices, are a top U.S. ICT export. They were the number three U.S. manufactured export over the last five years with 2014 sales of $172.9 billion.[47] U.S. ICT services are often inputs to final demand products that may be exported by other countries, such as China. 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 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.

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,[48] despite tariffs of up to 16% on these products.[49]

In 2014, Vietnam reportedly imported $10.3 billion worth of electronic integrated circuits (microchips) and associated parts, including approximately 4% or $398 million from the United States.[50] 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.[51]

Mexico and Vietnam are both members of the proposed Trans-Pacific Partnership (TPP) agreement (see below). If TPP enters into force, most ICT tariff lines would fall to zero for TPP partner countries. This would include the aforementioned radio equipment tariffs imposed on U.S. exporters by Vietnam, which would fall to zero by Year 4 of TPP's implementation.[52]

[45] OECD. (2015), OECD Digital Economy Outlook 2015, p. 38, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264232440-en.

[46] Angus Loten, "Trump Clouds Tech Spending Outlook," *The Wall Street Journal*, December 14, 2016.

[47] International Trade Administration, *2015 Top Markets Report Semiconductors and Semiconductor Manufacturing Equipment*," July 2015, http://trade.gov/topmarkets/pdf/Semiconductors_Top_Markets_Report.pdf.

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

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

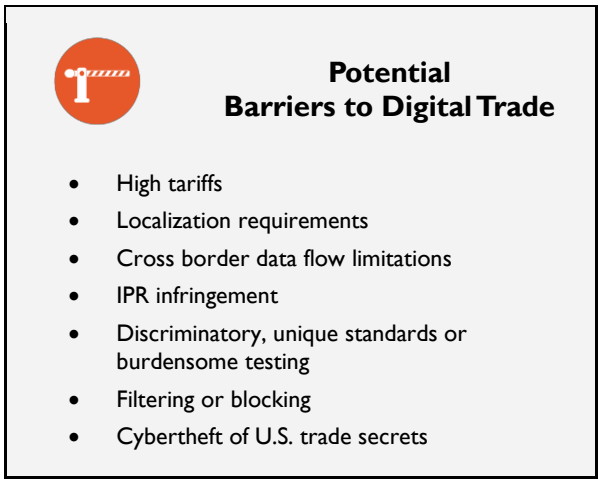
[50] U.S. Census Bureau.

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

[52] Trans-Pacific Partnership Annex 2-D: Vietnam Tariff Elimination Schedule, published by New Zealand Ministry of Foreign Affairs and Trade: https://www.mfat.govt.nz/assets/_securedfiles/trans-pacific-partnership/annexes/2-d.-viet-nam-tariff-elimination-schedule.pdf.

Nontariff Barriers

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



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

Broader governance issues, including rule of law, transparency, and investor protections, can pose barriers and limit the ability for firms and individuals to successfully engage in 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.[53] 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. Free trade agreements, such as the TPP, aim to ensure an open Internet and eliminate trade barriers while preserving flexibility for governments to pursue legitimate policy objectives (see below).

Cross-Border Data Flow Restrictions

Regulations limiting cross-border data flows 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.

Data localization requirements pose barriers to companies' efforts to operate more efficiently by migrating to the cloud. In 2014, 22% of businesses in OECD member countries used cloud

[53] 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.5-1, https://www.usitc.gov/publications/332/pub4415.pdf.

computing services, with higher use among large enterprises, and the number is accelerating.[54] For example, AT&T has said that it plans to move 80% of its applications into a private cloud by the end of 2016.[55] To better 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.[56] For companies more hesitant to embrace the cloud due to the security and regulatory concerns, Oracle Corp. has launched a hybrid cloud service offering.[57]

The Internet, and cloud services specifically, has been called the great equalizer, as 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.[58] 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 a USITC April 2015 report, the United States has the largest cloud computing industry globally (based on revenues) and 9 of the 10 largest cloud computing service providers (based on estimated number of servers).

Nevertheless, regulations or policies that limit data flows create barriers to firms and countries seeking to consume cloud services. As part of its submission to the U.S. Trade Representative (USTR) for the *2016 National Trade Estimate Report on Foreign Trade Barriers (NTE)*, for example, the Information Technology Industry Council (ITI) noted an increase in the use of forced localization measures, citing examples in China, Indonesia, Nigeria, Russia, Turkey, and Vietnam.[59] The Business Software Alliance's 2016 Global Cloud Computing Scorecard highlighted countries with improved policy environments but also those with localization requirements, particularly Russia's data protection framework (which contains prescriptive data localization requirements).[60]

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

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

[55] Rachael King, "AT&T to Move 80% of Its Applications to Cloud by Year's End," *The Wall Street Journal*, March 16, 2016, http://blogs.wsj.com/cio/2016/03/16/att-to-move-80-of-its-applications-to-cloud-by-years-end/.

[56] 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.

[57] Steve Rosenbush, "Oracle's New Service Turns Cloud Computing 'Inside-Out'," *The Wall Street Journal*, March 24, 2016.

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

[59] Information Technology Industry Council, *ITI Calls USTR Attention to Increasing use of Data Localization as a Trade Barrier and Threat to U.S. and Global Economic Growth*, October 29, 2015, http://www.itic.org/news-events/news-releases/iti-calls-ustr-attention-to-increasing-use-of-data-localization-as-a-trade-barrier-and-threat-to-u-s-and-global-economic-growth.

[60] Galexia Consulting, *2016 BSA Global Cloud Computing Scorecard*, Business Software Alliance, April 2016, http://cloudscorecard.bsa.org/2016/.

with a local company and transfer technology or intellectual property to that partner. Localization requirements can also pose a threat to intellectual property (discussed below).

Examples of Localization Barriers

Examples cited in 2016 National Trade Estimate Report on Foreign Trade Barriers (NTE):[61]

- In **Turkey**, a draft Personal Data Protection law would bar e-payment companies from the Turkish market if they do not have personal data banks located in Turkey.
- In **Nigeria**, the government issued guidelines for ICT products requiring multinational companies in Nigeria to source all hardware locally; use only locally manufactured SIM cards for telephone services and data; and use indigenous companies to build cell towers and base stations. The guidelines also require all government agencies to source and procure all computer hardware from government-approved original equipment manufacturers.
- 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.

Intellectual Property Rights (IPR) Infringement

Intellectual property rights (IPR)[62] are legal, private, enforceable rights that governments grant to inventors and artists; they generally provide right 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.[63] 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.[64] In 2015, U.S. charges for the use of IP (i.e., receipts of royalties and license fees) totaled about $125 billion, representing 17% of U.S. services exports, while U.S. payments for the use of IP (i.e., payments of royalties and license fees) totaled about $40 billion, representing about 8% of U.S. services imports.[65] 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**).

[61] Ambassador Michael B.G. Froman, *2016 National Trade Estimate Report on Foreign Trade Barriers*, Office of the United States Trade Representative, 2016, https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf.

[62] 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.

[63] 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.

[64] Ibid.

[65] CRS, based on U.S. Bureau of Economic Analysis (BEA), U.S. Trade in Services data, updated October 24, 2016. The charges for the use of IP reflect those not included elsewhere in BEA services data.

How Much IPR Infringement?

By its nature, IPR infringement is difficult to quantify, and estimates of its level and cost are sensitive to the assumptions made. Quantifying IPR infringement in the digital environment is all the more challenging given, for example, that "infringing files are traded online and websites offering counterfeits are launched and accessed, countless times each day."[66] 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 Organization for Economic Cooperation and Development (OECD) report estimates that trade in physically traded counterfeit and pirated goods totaled up to $461 billion (or 2.5% of world trade) in 2013, up from $200 billion (or 1.9% of world trade) in 2005 and $250 billion (or 1.8% of world trade) in 2007. The OECD analysis was based on custom seizures data (i.e., for goods seized at the border by countries' customs administrations), and did not include domestic IPR infringement or online piracy. However, a 2011 International Chamber of Commerce (ICC) study, building on OECD work, estimated that international trade in counterfeit and pirated products was $360 billion based on 2008 data, and as much as $960 billion when projecting to 2015. This study also pegged the value of digitally pirated music, movies, and software (not actual losses) as growing anywhere from $30-$75 billion based on 2008 data to $80-$240 billion when projecting to 2015. The FY2017-2019 *U.S. Joint Strategic Plan on Intellectual Property Enforcement* states that, taken together, the OECD and ICC studies "suggest that the total magnitude of counterfeiting and piracy worldwide in all forms appears to be approaching, if not surpassing, the trillion dollar mark."

Sources: USTR, *2016 Special 301 Report*, April 2016; OECD/EU Intellectual Property Office, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*, 2016; Frontier Economics, *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy*, report commissioned by Business Action to Stop Counterfeiting and Piracy (BASCAP) of the International Chamber of Commerce (ICC), February 2011; and *U.S. Joint Strategic Plan on Intellectual Property Enforcement: FY2017-2019*, December 2016.

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, 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."[67] IPR enforcement in the digital environment raises particular challenges.[68]

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. Cyber theft of trade secrets presents additional, increasingly prominent, barriers to digital trade.[69] Content industries say that IP theft costs them

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

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

[68] 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.

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

sales, takes away from legitimate services, harms investors in these businesses, damages their brand or reputation, and hurts "law-abiding" consumers.[70]

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. The use of illegal software by foreign governments is a particular concern.
- **Circumvention of technological protection measures (TPMs).** Measures such as encryption intended 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., cyber intrusions 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. China is a top concern in terms of cybertheft of trade secrets, but other countries, such as India, also present challenges. Key issues include gaps in these countries' trade secret laws and enforcement, including criminal penalties that are not sufficient to act as deterrents.
- **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, *2016 Special 301 Report*, April 2016 (designates countries that do not offer "adequate and effective" IPR protection and enforcement on various "watch lists"); USTR, *2016 Notorious Markets List*, December 2016 (identifies foreign websites operating as online markets reportedly involved in commercial-scale IPR infringement); and ITC, *Digital Trade in the U.S. and Global Economies, Part 1*, USITC Publication 4415, July 2013.

Identifying those responsible for IPR infringement is challenging. Companies in technology products and services sectors express concerns over unpredictable legal frameworks in foreign countries for online intermediary liability regarding infringing or illegal content transmitted over their systems. For example, they contend that foreign courts use outmoded Internet service provider (ISP) liability laws that impose substantial penalties on ISPs, which deter investment and market entry and, in turn, impede legitimate online services.[71] Countries identified by the USTR as having imposed liability in ways that are contrary to U.S. intermediary liability policy include France, Germany, Italy, India, and Vietnam.[72]

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,

[70] Ibid., p. 5-15.

[71] Computer & Communications Industry Association (CCIA), Comments to USTR in Response to Request for Public Comments to Compile the National Trade Estimate Report on Foreign Trade Barrier, 2015.

[72] Ibid.

they highlight and promote 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 right holder in certain cases, such as criticism, comment, news reporting, research, scholarship, and teaching.[73]

The USTR's *National Trade Estimate Report* similarly 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."[74]

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 hurts 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 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, customers in those markets have trouble accessing international providers.

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. If a company is required to provide the source code for ICT products to gain market access, it may fear theft of their IP and not enter that market (see above).

Filtering, Blocking, and Net Neutrality

Governments that filter or block websites, or otherwise impede access, form another type of non-tariff barrier. For example, China has asserted a desire for "digital sovereignty" and has erected what is termed by some as the "great firewall." A recent change to China's Internet filters also blocks virtual private network (or VPN) access to sites beyond the great firewall. Virtual private networks have been used by Chinese citizens to use websites like Facebook.[75] A rule issued by China's State Administration of Press, Publication, Radio, Film and Television and the Ministry of Industry and Information Technology bans all foreign media from publishing online. According to press reports, apart from select individual collaboration projects, only companies

[73] For more information on fair use, please see CRS Report RS22801, *General Overview of U.S. Copyright Law*, by Brian T. Yeh.

[74] USTR, *2016 National Trade Estimate Report on Foreign Trade Barriers*, p. 179, March 2016.

[75] Eva Dou, "China's Great Firewall Gets Taller," The *Wall Street Journal*, January 30, 2015.

that are 100% Chinese-owned will be able to produce online content, and only after approval from Chinese authorities and the acquisition of an online publishing license; foreign-owned or joint venture companies will be blocked from participating.[76]

According to recent press reports, Russia is now looking to emulate many of China's restrictive Internet practices.[77]

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" across the company's domains worldwide.[78] 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. In one critic's view, "France is trying to force its domestic policies on the rest of the world by coercing a global company that resides in its borders to implement those policies on all its users."[79] The conflict between Google and the EU authorities illustrate the complexity of the Internet and evolving technologies, and the lack of global standards that prevails in other areas of international trade.

National-level neutrality policies also differ widely. Net neutrality rules govern the management of Internet traffic as it passes over broadband Internet access services (BIAS), whether those services are fixed or wireless. In contrast to China, in the United States, the Federal Communications Commission (FCC) rules ban the blocking of legal content, forbid paid prioritization of content for consideration or to benefit an affiliate, and prohibit the throttling of legal content by BIAS providers.[80] In the EU, however, the Telecoms Single Market legislation allows providers to offer a zero rating and have discretion on managing traffic during times of network congestion, subject to regulator's approval.[81] As a result, each end user's access may be subject to the preferences and decisions of a telecom supplier.

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.[82]

Cyberattacks can pose broad risks to financial and communication systems, national security, privacy, and digital trade and commerce. Examples in the commercial sector include hacks into JPMorgan's systems in which customers' personal information was accessed, later blamed on Iran, and breaches of Sony Pictures Entertainment in which proprietary information and internal

[76] "Beijing is banning all foreign media from publishing online in China," *Quartz*, February 18, 2016.

[77] Max Seddon, "Russia's chief internet censor enlists China's know-how," *Financial Times*, April 26, 2016.

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

[79] Alan McQuinn, "France Demands Right to Censor the Global Internet," *The Innovation Files*, March 28, 2016.

[80] For more information on FCC rules on net neutrality, see CRS Report R43971, *Net Neutrality: Selected Legal Issues Raised by the FCC's 2015 Open Internet Order*, by Kathleen Ann Ruane, and CRS Report R40616, *The Net Neutrality Debate: Access to Broadband Networks*, by Angele A. Gilroy.

[81] Julia Fioretti. "EU regulators take tough approach to net neutrality," *Reuters*, June 2, 2016. Note: under a zero rating, a provider can exempt traffic from certain sites and services from a user's monthly data allowance.

[82] 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.

communications were stolen and exposed, later blamed on North Korea.[83] Another issue is that 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.[84]

U.S. Digital Trade with the EU and China

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 United States and EU policies have had 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, encompassing 46% of global GDP and 11% of the world's population.[85] Similarly, cross-border data flows between the United States and EU are the highest in the world. One estimate indicates that the United States exported $140.6 billion of digitally delivered services to the EU in 2012, which was 72% of total U.S. exports to the EU.[86] Many of these services are used to create further exports as part of GVCs. Of the digitally delivered services exported to the EU, 53% were incorporated into EU exports. In the opposite direction, the United States imported $86.3 billion of the same from the EU, 62% of which were incorporated into U.S. exports.[87] Furthermore, almost 40% of the data flows between the United States and EU are through business and research networks.[88]

Despite close economic ties, differences between the United States and EU in their approaches to data protection have caused friction in U.S.-EU economic and security relations. On October 6, 2015, the Court of Justice of the European Union (CJEU) invalidated the Safe Harbor Agreement under which personal data could legally be transferred between EU member countries and the United States. The decision was driven by European concerns that the U.S. approach to data privacy did not guarantee a sufficient level of protection for European citizens' personal data.

U.S. and EU officials announced the EU-U.S. Privacy Shield to replace the Safe Harbor agreement in early 2016, and it entered into force on July 12, 2016. The final agreement included additional obligations on the U.S. government, including a new ombudsman in the U.S. State

[83] Joseph Marks, "Indictment: Iranians made 'coordinated' cyberattacks on U.S. banks, dam," *Politico Pro*, March 24, 2016.

[84] 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.

[85] Based on Bureau of Economic Analysis (BEA), World Bank, and United Nations Committee on Trade and Development data.

[86] Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, Brookings, p.12, October 2014, http://www.brookings.edu/research/papers/2014/10/internet-transatlantic-data-flows-meltzer.

[87] Ibid, p. 17.

[88] 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.

Department and supplementary safeguards and limitations on surveillance, and on U.S. companies, such as robust data processing obligations. The Privacy Shield also involves proactive monitoring and enforcement by U.S. agencies, and is subject to an annual joint review by the United States and the EU.

The president of the French data protection authority (CNIL), Isabelle Falque-Pierrotin, stated that Privacy Shield is an opportunity to "build a common standard" between the EU and United States in cross-border data protection.[89] If the United States and EU are able to build a common standard, other parties may decide to adopt it, establishing a de facto global standard. Since then, the United States and Switzerland agreed to the Swiss-U.S. Privacy Shield, which will be "comparable" to the U.S.-EU agreement.[90] While companies are currently able rely on the Privacy Shield to ensure their digital data flows are allowed between the United States and EU, privacy advocates and others have begun to challenge the Privacy Shield in court which may, in turn, cause companies to hesitate enrolling in the program.[91]

EU Digital Regulations

As illustrated with the DPD (discussed above), EU policymakers are attempting to bring more harmonization across the region. Another initiative is 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 that is supported by 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, copyright 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, the United States has identified as a concern the Commission's consideration of a "duty of care" proposal as part of the DSM, which would "require some platforms to more proactively monitor and filter illegal content ... despite logistical difficulties and implications for free expression."[92] Concerns also arise from the Commission's May 2016 package of e-commerce proposals that contain an update of the Audiovisual Media Services Directive (AVMSD) that includes rules on platform liability and local content requirements.[93]

While the DPD set out common rules on how information about European citizens may be collected and used across all industries, each EU member state is responsible for implementing the Directive through its own national laws. To modernize the DPD and facilitate the creation of the DSM, EU member states (acting in the Council of the European Union) and the European Parliament reached political agreement in late 2015 on a new General Data Protection Regulation (GDPR).[94] In contrast to the DPD, the GDPR will be directly applicable in all EU member states, thus establishing a single set of rules (rather than harmonized ones) for data protection throughout the EU. However, one observer contends that there are still approximately 40 provisions that allow individual member states to set their own standards.[95]

[89] Daniel R. Stoller, "EU-U.S. Data Transfer Privacy Shield Opinion Imminent," *Bloomberg BNA*, April 5, 2016.

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

[91] *Inside U.S. Trade*, "Legal challenges against Privacy Shield begin to mount in Europe," November 3, 2016.

[92] USTR, *2016 National Trade Estimate Report on Foreign Trade Barriers*, p. 178.

[93] European Commission, "Commission updates EU audiovisual rules and presents targeted approach to online platforms," Press Release, May 25, 2016.

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

[95] Ali Qassim, "Lack of EU Data Reg Guidance Has Companies Uncertain," *Bloomberg BNA,* April 26, 2016.

The EU published the final GDPR on May 4, 2016; member states will have until May 25, 2018, to fully implement its provisions.[96] While the EU has begun to release guidance documents,[97] U.S. industry has voiced concern about the lack of clarity regarding some of the GDPR requirements and also about the potentially high penalties that may be imposed for violations (up to 2% of their annual worldwide revenues). Despite the lack of precise guidance, many companies have begun to analyze the regulation and plan for implementation. The potential impact of the GDPR on the EU-U.S. Privacy Shield is unclear, while the impact of the UK leaving the EU on either EU initiative is uncertain, although the UK's Information Commissioner supports amending UK data protection laws to meet the GDPR standards.[98]

These issues are likely to come up if the Transatlantic Trade and Investment Partnership (T-TIP) negotiations between the United States and EU resume under the Trump Administration. (See below.)

China

China presents a number of significant opportunities and challenges for the United States vis-a-vis digital trade. According to the Chinese government, at the end of December 2015, there were 688 million Internet users in China, including 620 million mobile Internet users. E-Marketer, a research firm that tracks digital issues, estimated China's e-commerce sales in 2014 totaled $672 billion (nearly double the U.S. level) and projected this would surge to $1.6 trillion by 2018.[99] E-Marketer also estimated that Chinese cross-border e-commerce sales would increase from $30.1 billion in 2014 to $85.8 billion in 2016, and by 2020 would reach $157.7 billion.[100] Although many U.S. firms may benefit from expanding digital trade in China, they may face numerous challenges as well.

Internet Governance

In December 2015, Chinese President Xi Jinping in a speech declared that the international community should respect the Internet sovereignty of individual countries in "choosing their own Internet development path, Internet governance, and Internet policies." To many observers, this represents a growing effort by the Chinese government to expand its control over the Internet in China in a way that could have negative consequences for U.S. firms attempting to do business in China, as well as for Chinese entrepreneurs.

The USTR's 2016 National Trade Estimates of Foreign Trade Barriers stated: "Over the past decade, China's filtering of cross-border Internet traffic has posed a significant burden to foreign suppliers, hurting both Internet sites themselves, and users who often depend on them for their businesses."

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 China's Internet market occurred in April 2016, when Chinese regulators, for

[96] Stephen Gardner, "Effective Date Set for EU General Data Protection Rule," *Bloomberg BNA*, May 4, 2016.

[97] Stephen Gardner, "First Guidance on New EU Privacy Law Will Help Companies," *Bloomberg BNA*, December 19, 2016.

[98] Ali Qassim, "U.K. Privacy Office Seeks EU-Compliant Laws Despite Brexit," *Bloomberg BNA*, July 5, 2016.

[99] E-Marketer, *Ecommerce Drives Retail Sales Growth in China*, September 25, 2015.

[100] E-Marketer, *China Embraces Cross-Border Ecommerce*, June 14, 2016, available at https://www.emarketer.com/Article/China-Embraces-Cross-Border-Ecommerce/1014078

unexplained reasons, suspended Apple iTunes Movies and iBooks Store, and DisneyLife services that had been operating in China for months.

IP Theft

China is considered by most analysts to be the largest source of global theft of IP. A May 2013 report by the Commission on the Theft of American Intellectual Property estimated that IP theft by Chinese entities annually cost the U.S. economy up to $240 billion. China is also considered to a major source of cybertheft of U.S. trade secrets, including by government entities. In May 2014, the United States Department of Justice indicted five members of the Chinese People's Liberation Army (PLA) for government-sponsored cyber espionage against U.S. companies and theft of proprietary information to aid state-owned enterprises (SOEs). In April 2015, President Obama issued an executive order authorizing certain sanctions against "persons engaging in significant malicious cyber-enabled activates."

Shortly before the arrival of Chinese President Xi's state visit to the United States, in September 2015, the Obama Administration indicated that it was considering imposing sanctions against Chinese entities over cybertheft, a move that likely could have led to a cancellation of Xi's visit. China sent a large delegation to the United States to discuss the issue, and during Xi's visit, the two sides reached an agreement whereby the two sides stated 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." The two sides also agreed to regularly hold high-level consultations on cyber issues (see textbox on the U.S.-China Cybersecurity Working Group).

New Restrictions on Information and Communications Technology

According to the USTR's 2015 report on China's WTO accession, while progress has been made to delink China's efforts on indigenous innovation from government procurement at the central and local levels, such policies have continued in other areas.

Many foreign business groups have expressed increasing concerns over a number of recently proposed or enacted laws and regulations on information and communications technology (ICT) products and services that could limit foreign access to ICT markets in China on so-called national security grounds. Several 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 lay out policies to promote indigenous ICT industries or would require 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.[101]

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

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.[102] Examples of recently passed or proposed measures of concern to foreign ICT firms include the following:

- In 2014, the China Banking Regulatory Commission issued guidelines for IT security equipment used in banks (such as for cash machines and smartcard chips), which included provisions on encryption and the disclosure of source code. The guidelines emphasized the importance of developing local technology and stated the need for "secure and controllable technologies" in the banking sector, with the goal of 15% in 2015, growing to no less than 75% in 2019. China suspended some of the guidelines in April 2015. At the June 2015 S&ED session, China agreed to ensure that bank ICT regulations "will be nondiscriminatory, are not to impose nationality-based requirements, and are to be developed in a transparent manner."[103]
- China's national security law (enacted in July 2015) emphasizes the State's role. It includes a provision (Article 24) that "the State strengthens the establishment of capacity for independent innovation, accelerating the development of autonomously controlled strategic advanced technologies and key technologies in core fields, strengthens the use of intellectual property rights, protects capacity building in protection of technological secrets, and ensures security in technology and engineering."[104] Article 59 says that "the State establishes national security review and oversight management systems and mechanisms, conducting national security review of 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."
- In October 2015, the China Insurance Regulatory Commission issued new draft rules on cybersecurity in the insurance industry. The draft rules called for the adoption of "secure and controllable" technology by insurance companies, data localization requirements, and the use of products and systems employing domestic encryption methods. On June 1, 2016, 28 business groups sent a letter to the chairman of the China Insurance Regulatory Commission, arguing that the draft rules "would create unnecessary obstacles to international trade and likely to constitute a means of arbitrary or unjustifiable discrimination against providers in countries where the same conditions prevail."[105] On June 2, 2016, the United States raised concerns about the draft regulations in the WTO Committee on Trade-Related Measures, arguing that such language appears to require that

[102] 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*, available at http://www.bea.gov/iTable/iTable.cfm?ReqID=62&step=1#reqid=62&step=1&isuri=1&6210=4.

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

[104] Translation from the Council on Foreign Relations, *National Security Law of the People's Republic of China*, July 1, 2015, available at http://www.cfr.org/homeland-security/national-security-law-peoples-republic-china/p36775.

[105] The letter can be found at https://www.uschina.org/sites/default/files/Industry%20letter%20on%20TBT%20notification%20of%20CIRC%20Tech%20Regulations%20(ENG).pdf.

Chinese insurance firms give preferences to Chinese domestic providers of hardware equipment and software over foreign firms.[106]

- In December 2015, China enacted a new counterterrorism law that requires telecommunications operators and Internet service providers to "provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities."[107] Originally, the Chinese government sought to require operators to provide encryption codes (i.e., security back-door access) and to store local user data on servers within China, but these provisions were dropped in the final draft of the law, in part because of sharp criticism by President Obama, who contended that such rules "would essentially force all foreign companies, including U.S. companies, to turn over to the Chinese government mechanisms where they can snoop and keep track of all the users of those services."
- China passed a new cybersecurity law on November 7, 2016, which appears to promote the development of indigenous technologies and impose restrictions on foreign firms.[108] Article 15 directs government entities to "support key network security technology industries and programs; support network security technology research and development, application and popularization; spread safe and trustworthy network products and services; protect the intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, and so forth to participate in State network security technology innovation programs." Article 23 states that "Critical network equipment and specialized network security products shall follow the national standards and mandatory requirements, and be safety certified by a qualified establishment or meet the requirements of a safety inspection, before being sold or provided. The state network information departments, together with the relevant departments of the State Council, formulate and release a catalog of critical network equipment and specialized network security products, and promote reciprocal recognition of safety certifications and security inspection results to avoid duplicative certifications and inspections."[109] Article 37 states that personal information and other important data gathered or produced by critical information infrastructure operators during operations within China must be stored in China. A statement issued by Amcham on November 7 said the new law would not "do much to improve security," but rather, "create barriers to trade and investment." Other critics contend that provisions of the law are too broad or vague as to the level of cooperation Internet firms are required to give to government authorities and would impose new Internet restrictions.[110]

[106] Inside U.S. Trade's, China Trade Extra, "U.S. Signals It Wants China To Slow Implementation Of Draft Insurance Regs," June 3, 2016.

[107] A translated copy of the law can be found at the China Law Translate at http://chinalawtranslate.com/?lang=en.

[108] The law follows China's assertion of its right to "cyber-sovereignty, which it describes as "an individual country's right to choose its own Internet regulation model." See Xinhuanet, "China Voice: Why does cyber-sovereignty matter?," December 12, 2016, available at http://news.xinhuanet.com/english/2015-12/16/c_134923687.htm.

[109] See translation of the law at http://chinalawtranslate.com/cybersecuritylaw/?lang=en#LBQMwbmaWhGozeMj.99.

[110] Lawfare, *Understanding China's Cybersecurity Law*, November 8, 2016, available at https://www.lawfareblog.com/understanding-chinas-cybersecurity-law.

In May 2017, 53 international business groups sent a letter to the Chinese government, asking it to delay implementation of its new cybersecurity law, noting concerns over provisions that restrict of cross-border data flows, impose forced technology requirements on foreign firms, impose trade-inhibiting security reviews and requirements for ICT products and services, and establish broad requirements for data sharing and technical assistance. While many multinational companies have continued to voice concern about the lack of clarity of the law's requirements, most aspects of the cybersecurity law went into force on June 1, 2017, with the Cyberspace Administration of China beginning to conduct national security reviews on technology suppliers.[111] China did postpone the implementation of the cross-border data flow restrictions, giving companies until the end of 2018 to comply.

- China's recent five-year plans and other government policy pronouncements have laid out a number of plans to boost innovation and promote the development of indigenous ICT and other high-tech sectors, including semiconductors (see Appendix 1).

A 2016 U.S.-China Business Council survey found that 79% of respondents are concerned about China's data and IT security policies, including the impact they have on day-to-day business operations. 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% up to 3.44%, or at least $200 billion (based on 2015 GDP), and would cost the economy at a minimum nearly $3 trillion overall by 2025.[112]

U.S.-China BIT Negotiations

In 2008, the United States and China launched negotiations for a bilateral investment treaty (BIT), an agreement that typically contains provisions to encourage and provide reciprocal investment protections in order to enhance bilateral commercial ties. In 2013, China agreed to negotiate a "high standard" BIT with the United States, which would include opening new sectors to FDI and generally treating U.S.-invested firms in China the same as Chinese firms. China agreed to negotiate investment liberalization on a negative list basis, meaning only those industries listed in the agreement would be closed off to foreign investment—all other sectors would be open. Many analysts contend that a BIT could significantly boost bilateral FDI and trade flows. Such an agreement, if concluded, might provide significant new opportunities for U.S. firms that are engaged in digital trade.[113] However, the USTR's 2016 report on China's WTO compliance indicated that while China has been fully engaged in the BIT negotiations, it "has not yet decided to pursue a sufficient reduction of its investment restrictions to enable the successful conclusion of those negotiations."[114] It is unclear if the BIT talks will continue under the Trump Administration.

---

[111] Eva Dou, "China to Start Security Checks on Technology Companies in June," *Wall Street Journal*, May 3, 2017, https://www.wsj.com/articles/china-to-start-security-checks-on-technology-companies-in-june-1493799352.

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

[113] For more information on U.S. China trade relations and the BIT negotiations, see CRS In Focus IF10030, *U.S.-China Trade Issues*, by Wayne M. Morrison, and CRS In Focus IF10307, *A U.S.-China Bilateral Investment Treaty (BIT): Issues and Implications*, by Wayne M. Morrison.

[114] USTR, *2016 Report to Congress on China's WTO Compliance*, January 2017, p. 4, available at https://ustr.gov/sites/default/files/2016-China-Report-to-Congress.pdf.

U.S.-China Cybersecurity Working Group

As a result of the 2015 S&ED meeting and cybersecurity agreement, the United States and China established U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues.[115] According to the White House, the group "will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side." The group first met in December 2015 and agreed on guidelines, conducting a tabletop exercise, a hotline mechanism, and enhanced cooperation on cyber-enabled crime.[116] At the second meeting in June 2016, the parties agreed to a second tabletop exercise, implementation of the hotline, cooperation in network protection, information sharing, and the first U.S.-China Senior Experts Group on International Norms in Cyberspace and Related Issues. They also agreed to cooperate on investigations, combatting IP theft, and law enforcement operations in specific areas.[117] The third working group meeting took place on December 8, 2016. Discussions were held on combatting cybercrime and cyber-enabled crime, network protection, misuse of technology and communications to facilitate violent acts of terrorism, and the operation of the U.S.-China Cybercrime and Related Issues Hotline Mechanism. It is unclear what effect the dialogue has had on Chinese cyber-theft of U.S. trade secrets. Some have speculated that, given the importance of cyber issues, the bilateral cyber working group will likely continue into the Trump Administration.[118]

As negotiations with each of the EU and China demonstrate, there no single international standard that governs digital data flows, and the topic is treated inconsistently, if at all, in trade agreements.

A United Nations Conference on Trade and Development (UNCTAD) report exploring data protection pointed out that differences in social and cultural norms affect if, and how, countries regulate privacy, which in turn can have trade implications.[119] In reviewing privacy and data flow regimes at national and regional levels globally, UNCTAD identified common core principles: openness, collection limitation, purpose specification, use limitation, security, data quality, access and correction, and accountability.[120] The report urges global work toward an agreement or mechanism to promote international harmonization or compatibility between the different regimes. After all, "(c)reating trust online is a fundamental challenge to ensuring that the opportunities emerging in the information economy can be fully leveraged."[121]

Despite common core principles, governments face multiple challenges in designing policies. 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.[122]

---

[115] The White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," September 25, 2015.

[116] U.S. agencies included the Departments of Justice, Homeland Security, and State and the National Security Council and Intelligence Community and while Chinese representatives came from the Committee of Political and Legal Affairs of CPC Central Committee, Ministry of Public Security, Ministry of Foreign Affairs, Ministry of Industry and Information Technology, Ministry of State Security, Ministry of Justice and the State Internet Information Office. Department of Justice, "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes," December 2, 2015.

[117] Department of Homeland Security, "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," June 15, 2016.

[118] Cory Bennett, "U.S., China cyber talks will continue into Trump administration," *Politico Pro*, December 8, 2016.

[119] United Nations Conference on Trade and Development, *Data protection regulations and international data flows: Implications for trade and development*, 2016, http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

[120] Ibid, p. 56.

[121] Ibid, p. xi.

[122] 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.

Digital Trade Provisions in Trade Agreements

As digital trade has emerged as an important component of trade flows, it has risen in significance on the trade policy agenda of many countries, including the United States. Given the current stalemate in the WTO Doha Round negotiations, multilateral trade agreements have not kept pace with the complexities of the digital economy and digital trade is treated unevenly, if at all, in existing WTO agreements. More recent bilateral and plurilateral deals have started to address digital trade 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.

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.[123]

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 10th Ministerial Conference of the WTO, in December 2015, concluded with no clear path forward for the Doha Development Agenda (DDA), reflecting an ongoing wide division among members. Most developing countries want to continue the DDA round that links the broad spectrum of agricultural and nonagricultural issues, maintaining that unless all issues are addressed in a single package, issues important to developing countries will be ignored.

Conversely, advanced economies, including the United States and EU, have pushed for an end to the long-stalled round, arguing that the Doha agenda has proven untenable and that a different approach is needed in order to address new issues including e-commerce and data flows. While members claim to remain committed to addressing the outstanding issues of the round, both agricultural and nonagricultural, the Nairobi Ministerial Declaration acknowledged the division over the future of the Doha Round, and failed to reaffirm its continuation, leaving its future uncertain.[124]

[123] 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.

[124] For more information on WTO and the Doha Round, see CRS In Focus IF10002, *The World Trade Organization*, by Ian F. Fergusson and Rachel F. Fefer.

Information Technology Agreement (WTO ITA)

The World Trade Organization (WTO) Information Technology Agreement (ITA) aims to eliminate tariffs on the goods that power and utilize the Internet. 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 will eliminate tariffs on 201 additional IT products valued at over $1.3 trillion per year.[125] The increased coverage includes, for example, many consumer electronics, new generation semi-conductors (multi-component semiconductors, or MCOs), and medical instruments like magnetic resonance imaging (MRI). According to the U.S. Trade Representative (USTR), the agreement will provide duty-free access to $180 billion in annual U.S. exports.[126] 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.

While the WTO ITA is expected to expand trade in the technology products that underlie digital trade, it does not tackle the nontariff barriers that can pose significant limitations.

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."[127] The 1998 declaration establishing the program also included a statement that "members will continue their current practice of not imposing customs duties on electronic transmission."[128]

Reflecting the lack of agreement in the final WTO Ministerial Declaration, the latest report for the work program stated that there was not consensus on how to move forward beyond the information sharing stage to identify specific outcomes or recommendations.[129] In the draft decision in November 2015, members agreed to continue periodic reviews of the work program, the current moratorium on customs duties on electronic transmissions, and having the other WTO bodies explore the relationship between existing WTO agreements and e-commerce based on proposals submitted by members.[130]

---

[125] 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.

[126] 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.

[127] "Exclusively for the purposes of the work programme, and without prejudice to its outcome, the term 'electronic commerce' is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means."

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

[129] For more information on the Work Programme on Electronic Commerce, see https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm and https://www.wto.org/english/thewto_e/minist_e/min99_e/english/about_e/20ecom_e.htm.

[130] https://www.wto.org/english/news_e/news15_e/gc_30nov15_e.htm.

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

The TRIPS Agreement, signed on April 15, 1994, and 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.[131]

TRIPS aims to balance rights and obligations between protecting private right holders' interests and securing broader public benefits. It includes provisions on

- WTO nondiscrimination principles (national treatment and most-favored-nation);
- minimum standards of protection for IPR, such as copyright protection terms for the life of the author plus 50 years;
- minimum standards of enforcement of IPR through civil actions for infringement, border enforcement, and criminal actions;
- applying the WTO's binding Dispute Settlement Mechanism to IPR disputes; and,
- requiring developed countries to provide incentives for technology transfers to LDCs "to enable them to create a sound and viable technological base."

Among other 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.[132]

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

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

[132] 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.

protection and enforcement of copyright and related rights, trademarks, and new technologies and access to these technologies.[133]

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 under WTO dispute settlement. Shaped by TRIPS, the WIPO Internet Treaties are intended to clarify that existing rights continue to apply in the digital environment, to create new online rights, and to maintain a fair balance between the owners of rights and the general public.[134]

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. An "agreed statement" regarding Article 8 of the WIPO Copyright Treaty sought to clarify the issue by providing that "the mere provision of physical facilities for enabling or making a communication [e.g., wires, telephone lines, modems] does not in itself amount to communication within the meaning of this Treaty or the Berne Convention...." The WIPO Internet Treaties leave it to the discretion of national governments to develop the legal parameters for Internet Service Provider (ISP) liability.[135]

As of April 2016, the WIPO Internet Treaties had 94 contracting parties. The United States implemented the WIPO Internet Treaties through the Digital Millennium Copyright Act of 1998 (DMCA), which set new standards for protecting copyrights in the digital environment, including prohibiting the circumvention of anti-piracy measures incorporated into copyrighted works and enforcing such violations through civil, administrative, and criminal remedies.[136] 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."[137] The United States has continued to call on trading partners, such as Canada and Mexico, to fully implement the WIPO Internet Treaties.[138]

---

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

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

[135] 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.

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

[137] 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.

[138] USTR, *2016 Special 301 Report*, April 2016.

Future Sectoral Approaches

With the stalling of the Doha Round of negotiations, WTO members and experts have raised various options to address emerging issues such as digital trade. Ideas include the following:

- Updating the rules within the WTO framework to address digital trade.[139] Options could include expanding the multilateral GATS to cover cross-border data flows, technology transfer, or greater market access issues. Others support using the existing plurilateral WTO ITA, Telecommunications, or the Trade Facilitation Agreement to address digital trade and tackle barriers ranging from tariffs to express delivery and mobile services.
- Establishing a permanent WTO working group dedicated to exploring digital issues, possibly based on the current Work Programme, or to create a new stand-alone trade agreement specific to data services or digital trade, possibly initially as an open plurilateral deal.
- Creating a separate digital trade-specific WTO agreement, an "e-WTO" as some have suggested. USTR Ambassador Froman noted that "[n]ew rules on critical 21st century issues, such as e-commerce and the digital economy, are emerging.... a better path forward is a new form of pragmatic multilateralism. Moving beyond Doha doesn't mean leaving its unfinished business behind. Rather, it means bringing new approaches to the table."[140]

In July 2016, the United States put forward a submission under the WTO Work Programme on Electronic Commerce offering "trade-related policies that can contribute meaningfully to the flourishing of trade through electronic and digital means" but without specific negotiating proposals.[141] The 16 policies included in the U.S. submission align with the proposed Trans-Pacific Partnership (see below), such as prohibiting digital customs duties and enabling cross-border data flows. The policies focus on eliminating or preventing trade barriers and establishing a transparent, adaptable framework for digital trade. The policies also recognize the need for balancing digital trade with other priorities such as protection of consumer data, security, and law enforcement.[142]

Similarly, China put forward a proposal in November 2016 in which it seeks "to clarify and to improve the application of existing multilateral trading rules" with a focus on facilitating e-commerce.[143]

U.S. Bilateral and Plurilateral Agreements

As discussed above, the WTO agreements provide limited treatment of some aspects of digital trade. The stalled Doha Round 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

[139] Joshua Paul Meltzer, *Maximizing the Opportunities of the Internet for International Trade*, The E15 Initiative, January 2016, http://e15initiative.org/publications/maximizing-opportunities-internet-international-trade/.

[140] Michael Froman, "We are at the end of the line on the Doha Round of trade talks," *Financial Times*, December 13, 2015.

[141] WTO, "Non-Paper from the United States," JOB/GC/94, July 4, 2016.

[142] Ibid.

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

outside of the WTO. The United States has included, and continues to expand on, digital trade provisions 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.[144] 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.[145] Most chapters contain provisions on nondiscrimination of digital products, prohibition of customs duties, transparency, and cooperation topics such as SMEs, cross-border information flows, and promoting dialogues to develop e-commerce. Some of the FTAs also include cooperation on consumer protection, as well as providing for electronic authentication and paperless trading. All FTAs allow certain exceptions to ensure that each party is able to achieve legitimate public policy objectives, protecting regulatory flexibility.

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

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

The U.S.-South Korea FTA (KORUS) contains the most robust digital trade provisions in a U.S. FTA currently in force.[146] 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 mention explicitly 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."[147]

The Proposed Trans-Pacific Partnership (TPP) Agreement

The Trans-Pacific Partnership (TPP) is a proposed FTA among 12 Asia-Pacific countries, including both developed and developing countries. The agreement has economic and strategic significance for the United States and was officially signed on February 4, 2016.[148] Congress must pass implementing legislation before the TPP agreement can take effect in the United States. In considering TPP, Congress may weigh whether the agreement makes enough progress in achieving the TPA negotiating objectives on digital trade to merit passage of implementing legislation.

---

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

[145] 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.

[146] 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.

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

[148] For more on TPP, see CRS In Focus IF10000, *TPP: Overview and Current Status*, by Brock R. Williams and Ian F. Fergusson, CRS Report R44489, *The Trans-Pacific Partnership (TPP): Key Provisions and Issues for Congress*, coordinated by Ian F. Fergusson and Brock R. Williams, and CRS In Focus IF10390, *TPP: Digital Trade Provisions*, by Rachel F. Fefer.

The proposed TPP goes beyond the digital trade 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 of the TPP (e.g., e-commerce, financial services, telecommunications, technical barriers to trade, intellectual property rights), showing the complexity of digital trade barriers and issues. The TPP encourages parties to become members of the tariff-eliminating WTO Information Technology Agreement. In reviewing the TPP, the Industry Trade Advisory Committee on Information and Communication Technologies Services and Electronic Commerce (ITAC 8) endorsed the agreement, finding that the TPP promotes the economic interests of the United States, and provides equity and reciprocity for the sectors represented by the ITAC.[149]

The proposed TPP has several digital trade-related innovations, including:

- Prohibits cross-border data flow restrictions and data localization requirements, except for financial services and government procurement.
- Prohibits requirements for source code disclosure or transfer as a condition for market access, with exceptions.
- Requires parties to have online consumer protection and anti-spam 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.

In addition to excluding government procurement, TPP allows for exceptions to its digital trade commitments to achieve legitimate public policy goals such as protecting health, safety, and national security. Like other FTAs, the TPP also includes annexes of nonconforming measures in which each country negotiates to exclude specific regulations, laws, or sectors from its agreement obligations. For example, Japan includes national security screening requirements on "telecommunications and internet based services."[150] Unless a country takes an exception through a nonconforming measure, the "negative" list approach of TPP would ensure that new services or innovations would be covered under the agreement obligations.

For the first time, TPP would require parties to have a legal framework to protect personal information. TPP critics contend that the provisions are vague and do not contain an explicit

[149] Industry Trade Advisory Committee on Information and Communication Technologies, Services, and Electronic Commerce (ITAC 8), *Advisory Committee Report to the President, the Congress and the USTR on the TPP Trade Agreement*, December 3, 2015, https://ustr.gov/sites/default/files/ITAC-8-Information-and-Communication-Technologies-Services-and-Electronic-Commerce.pdf.

[150] Annex I for Japan includes Foreign Exchange and Foreign Trade Law (Law No. 228 of 1949), Article 274 Cabinet Order on Foreign Direct Investment (Cabinet Order No. 261 of 1980), Article 3, https://ustr.gov/sites/default/files/TPP-Final-Text-Annex-I-Non-Conforming-Measures-Japan.pdf.

minimum standard for privacy protection. Supporters note that TPP includes a reference to take into account "guidelines of relevant international bodies" that may include the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[151]

While most industry advocates support TPP, critics point out that financial services are not covered by the overall e-commerce chapter. The financial services chapter, instead, includes a separate provision covering cross-border data flows based on the language in KORUS, but it does not contain a prohibition on localization requirements similar to the e-commerce chapter.[152]

On November 21, 2016, President-elect Donald Trump announced his intent to withdraw from the proposed TPP once in office.[153]

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, with a goal of concluding the agreement in 2017.[154] 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.

While nondiscrimination (MFN) applies to all services sectors, in TiSA, unlike TPP, market liberalization commitments are being negotiated under a hybrid approach. That is, specific market access obligations to liberalize service markets are being negotiated under a positive list in which parties "opt in" specific service sectors, while national treatment obligations are being negotiated under a negative list (in which parties may "opt out" certain sectors or sub-sectors). The positive list may be viewed as less ambitious because new inventions or sectoral innovations would not be covered under TiSA unless they are explicitly added in the future, a potential concern in the quickly evolving world of digital trade.

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.[155] 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 non-discrimination obligations.[156]

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

[151] TPP Chapter 14, Article 14.8.2.

[152] For more, see CRS In Focus IF10390, *TPP: Digital Trade Provisions*, by Rachel F. Fefer.

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

[154] 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.

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

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

language that is open enough to enable trade and address evolving technology, but concrete enough for regulators to protect privacy and safeguard cybersecurity. While technical discussions continue, negotiations are on pause until the Trump Administration decides how it wishes to proceed.

Transatlantic Trade and Investment Partnership (T-TIP) Negotiations

T-TIP is a potential FTA that the United States and the EU began negotiating in 2013 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. Digital trade is a key area of interest because of its significance to transatlantic trade. Services that can be delivered over the Internet constitute the majority of U.S. and EU services exports to each other.[157] Presently, T-TIP negotiations are on pause until the Trump Administration decides how it wishes to proceed.

If negotiations continue, T-TIP could address digital trade issues in a number of areas. In addition to provisions to provide enhanced market access for digital products,[158] a potential T-TIP could include commitments addressing non-tariff barriers to digital trade. Provisions on regulatory cooperation could include both sector-specific commitments (e.g., for the ICT sector) and horizontal commitments (e.g., on stakeholder input, transparency). The United States and the EU have "different legal traditions, regulatory paths, market outcomes," and policymaking approaches that constrain integration of a transatlantic digital economy. Another area of focus could be enhanced rules and disciplines governing digital trade, such as commitments on facilitating data flows across borders and addressing localization requirements (e.g., data storage or server location requirements). Other features of a potential T-TIP could include rules to protect and enforce IPR, including copyrights, balanced against limitations on ISP liability and "fair use" exceptions. Such IPR rules could protect against forced transfers of source code, or establish criminal procedures for cyber theft, among other things.

U.S.-EU engagement on digital trade issues in a potential T-TIP may be complicated or influenced by a number of other factors, such as the EU's "Digital Single Market" initiative, new and revised EU policies on data protection, the EU-U.S. Privacy Shield implementation, and the UK's decision to leave the EU ("Brexit"). Digital trade issues also may be a focal point in any potential future bilateral FTA negotiations between the United States and UK.

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 instill firm obligations with trading partners, 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

[157] Ibid.

[158] Under the Obama Administration, a U.S. goal for T-TIP has 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.

forums outside of trade negotiations, other tools can be used to encourage high-level, non-binding 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 their agenda recently.[159] At their November 2015 meeting, the G-20 leaders issued a statement that included new provisions on the Internet economy, recognizing the opportunities and challenges presented to global economic growth and development, affirming not to conduct or support ICT-enabled IP theft for commercial competitive advantage, and acknowledging the need to respect and protect privacy.[160] China is the 2016 host for the G-20 and selected the theme "Towards an Innovative, Invigorated, Interconnected and Inclusive World Economy," opening the opportunity for further conversation on the digital economy and the chance to set global norms.

G-7. The G-7 ICT Ministers met in Japan in April 2016 and issued a Joint Declaration, stressing principles including the importance of investment in infrastructure, digital literacy, and accessibility; promoting cross-border data flows, privacy and data protection, and cybersecurity; and fostering innovation through open markets, interoperable standards, protecting IP, and facilitating research and development.[161] The United States could work with G-7 partners to incorporate these principles into the broader G-20.

OECD. The OECD offers yet another forum to discuss principles and norms to ensure 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.

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.[164] 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 developing and implementing

[159] 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.

[160] http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

[161] Joint Declaration by G7 ICT Ministers, April 30, 2016, http://www.g8.utoronto.ca/ict/2016-ict-declaration.html.

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

a Cross-Border Privacy Rules system to be consistent with the already established APEC Privacy Framework.[165] 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. As such, by maintaining U.S. involvement in APEC, the United States can guide efforts to establish principles and norms in the region and subsequent roll-out worldwide.

Regulatory cooperation. Congress could consider having U.S. regulatory agencies that cover specific aspects of digital trade (e.g., U.S. Federal Trade Commission, Customs and Border Protection) work with overseas counterparts to better align regulatory requirements and reduce inconsistencies and redundancies that can hamper or discriminate against the free flow of data, goods, and services. Online privacy, consumer protection across borders, and rules for online contract formation and enforcement are potential areas for regulatory cooperation. The EU-U.S. Privacy Shield is one example of regulatory authorities working together to address such issues.

Policy 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, are concerned with maintaining open market access, which may include cross border data flows, while others may want to limit foreign competition. Privacy advocates 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:

- Understanding of the economic impact of digital trade on the U.S. economy and the effects of localization and other digital trade barriers on U.S. exports, jobs, and competition.
- Examining how best to balance an individual's right to privacy for conduct online 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.
- Reviewing what government policies to pursue with the private sector to support innovation and economic growth in digital trade both domestically and internationally.

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

- Examining the evolving U.S. trade policy efforts including the EU-U.S. Privacy Shield, proposed TPP, and WTO policy principles to determine if these mechanisms establish an appropriate balance among public policy objectives, and conducting oversight of implementation should they enter into force.
- Assessing if China is abiding by its commitments in the bilateral cyber agreement and on market access for U.S. ICT firms, as well as the effectiveness of the bilateral cyber dialogue.
- Reviewing federal-level efforts related to digital trade, such as the Department of Commerce's Digital Economy Agenda or infrastructure programs, and determining if changes to current plans or funding levels are needed.
- Conducting oversight of federal agencies in terms of roles and competencies related to digital trade, such as those organizations charged with coordinating federal efforts on IPR or law enforcement; trade negotiations and enforcement; and cybersecurity.

Author Contact Information

Rachel F. Fefer, Coordinator
Analyst in International Trade and Finance
rfefer@crs.loc.gov, 7-1804

Shayerah Ilias Akhtar
Specialist in International Trade and Finance
siliasakhtar@crs.loc.gov, 7-9253

Wayne M. Morrison
Specialist in Asian Trade and Finance
wmorrison@crs.loc.gov, 7-7767

Acknowledgments

Special acknowledgement to Gabriel Nelson for tariff research and to Amber Wilhelm for creation of the graphics.