Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Rachel F. Fefer
Analyst in International Trade and Finance

Before

Joint Economic Committee
U.S. Joint Committee

Hearing on

"The Need for U.S. Leadership on Digital Trade"

June 21, 2018

Congressional Research Service
7-5700
www.crs.gov
<Product Code>

CRS TESTIMONY
Prepared for Congress

Search Terms

Trade barriers

Digital trade

Cross border data flows

Localization

International trade

General Data Protection Regulation

GDPR

Chairman Paulsen, Ranking Member Heinrich, and Members of the Joint Economic Committee, thank you for the opportunity to appear before you today on behalf of the Congressional Research Service to discuss "The Need for U.S. Leadership on Digital Trade." My name is Rachel Fefer and I am an Analyst in International Trade at the Congressional Research Service. As requested, my testimony focuses on the possible implications of the increase in digital trade barriers across the globe and how other countries are attempting to set new international standards and rules that may impact market access for U.S. companies and U.S. consumers.

What is Digital Trade?

The internet-driven digital revolution is causing fundamental change to the U.S. and global economy, leading to new modes of communication and information-sharing, business models, sources of job growth and changes to the composition of jobs, and to new policy challenges. Digital technology enables the creation of new goods and services, including, for example, e-books, online education, and online banking services. Digital technology may also affect the production process for traditional goods and services, raising productivity and/or lowering the costs and barriers related to trade flows, such as for supply chain tracking, 3-D printing, or devices or objects connected via the Internet of Things. Digital platforms serve as intermediaries for multiple forms of digital trade, including e-commerce (e.g., eBay), social media (e.g., Facebook), and cloud computing (e.g., Amazon web services). In these ways, digitization pervades every industry sector, creating challenges and opportunities for established and new players.

The increase in digital trade parallels the growth in internet usage globally. Cross-border data and communication flows are part of digital trade; they also facilitate trade and the flow of goods, services, people, and finance, which together are the drivers of globalization and interconnectedness. One estimate shows that although cross-border bandwidth increased 45-fold from 2005 through 2015, it may still grow nine times larger by 2021.[1]

While there is no globally accepted definition of digital trade, the U.S. International Trade Commission (USITC) broadly defines digital trade as follows:

> The delivery of products and services over the Internet by firms in any industry sector, and of associated products such as smartphones and Internet-connected sensors. While it includes provision of e-commerce platforms and related services, it excludes the value of sales of physical goods ordered online, as well as physical goods that have a digital counterpart (such as books, movies, music, and software sold on CDs or DVDs).[2]

The Importance of Digital Trade to the U.S. and Global Economy

In 2016, the digital economy supported 5.9 million U.S. jobs, or 3.9 percent of total U.S. employment, and accounted for 6.5% of current dollar Gross Domestic Product (GDP).[3] Workers in the digital economy earned average annual compensation of $114,275 compared to the economy-wide average of

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

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

[3] Digital economy here is defined primarily in terms of the Internet and related information and communications technologies (ICT), including (1) the digital-enabling infrastructure needed for a computer network to exist and operate, (2) the digital transactions that take place using that system ("e-commerce"), and (3) the content that digital economy users create and access ("digital media"). Source: Kevin Barefoot, Dave Curtis, William Jolliff, Jessica R. Nicholson, Robert Omohundro, *Defining and Measuring the Digital Economy*, U.S. Bureau of Economic Analysis (BEA), March 15, 2018.

$66,498.[4] Four U.S. firms (Amazon, Microsoft, Google, and IBM) were the top global providers of cloud services in 2016.[5]

The USITC estimated global e-commerce to be worth $28 trillion in 2016, of which 86 percent was business-to business activity.[6] Global e-commerce grew by an estimated 44 percent over the past five years. Information and communication technology (ICT) services, a relative U.S. competitive strength, are outpacing the growth of international trade in ICT goods. The United States is the fourth-largest Organization for Economic Co-operation and Development (OECD) exporter of ICT services.[7] ICT-enabled services are those services with outputs delivered remotely over ICT networks, such as online banking or education, and can augment the productivity and competitiveness of goods and other services. In 2016, exports of ICT services totaled $66 billion of U.S. exports while services exports that could be potentially ICT-enabled were another $404 billion, demonstrating the impact of the internet and digital revolution.[8] As digitization is integrated into the broader economy, digital trade could increasingly become the underlying facilitator of many aspects of traditional international commerce.

Digital Trade Barriers

As noted in your committee's *2018 Economic Report of the President*, "Digital trade has been growing rapidly in recent years," but "challenges to the smooth international flow of goods and funds may prevent trade from reaching its most efficient level."[9]

The increase in digital trade raises new challenges in U.S. trade policy, including how best to address new and emerging trade barriers. Protectionist policies can create barriers to digital trade, or damage trust in the underlying digital economy. This could result in fragmenting the internet, lessening any potential gains by limiting organizations' or individuals' access to markets or data. Governments must often attempt to balance a number of legitimate policy objectives related to digital trade including ensuring national security, promoting innovation and competition, and guaranteeing citizens privacy. However, legitimate policy objectives may also be cited as a rationale for actions that are actually intended to protect the domestic market from international competition. The OECD points out three potentially conflicting policy goals in the internet economy: (1) enabling the internet through regulation without hindering innovation; (2) boosting or preserving competition within and outside the internet; and (3) protecting privacy and consumers more generally.[10]

The U.S. policy, as stated in President Trump's National Security Strategy, is to "advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services" and "promote the free flow of data."[11] Foreign digital trade barriers are specifically recognized in the U.S. Trade Representative (USTR)'s annual National Trade Estimate Report.[12] The report identifies a number

[4] Ibid.

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

[6] Ibid.

[7] In 2016, the largest exporters of ICT services were Ireland, India, and the Netherlands. OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-en.

[8] Bureau of Economic Analysis (BEA), https://bea.gov/scb/pdf/2017/10-October/1017-international-services-tables.pdf.

[9] U.S. Congress, Joint Economic Committee, *The 2018 Joint Economic Report*, committee print, 115th Cong., 2nd sess., March 13, 2018, 115-596, p. 48.

[10] 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.

[11] The President of the United States, "National Security Strategy of the United States of America," December 2017.

[12] https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

of individual country policies across the globe that may impact U.S. digital trade, illustrating the breadth and variety of digital trade barriers (see **Figure 1**). Digital trade barriers, many of which are highlighted in the report, include:

- **High tariffs**. Tariffs on ICT or digital goods or services may raise costs for sellers and potentially result in higher prices for buyers. Though World Trade Organization (WTO) agreements and U.S. free trade agreements (FTAs) eliminate tariffs on most ICT goods and digital trade, some countries have considered tariffs to raise revenue and protect domestic industries.[13] Exemption from duties and simplified customs procedures for low-value shipments (i.e., a *de minimus* threshold) can facilitate trade and expand e-commerce exports. Raising *de minimus* levels may be especially important for U.S.-based small and mid-sized enterprises (SMEs) seeking to export, because the United States has a relatively high *de minimus* threshold ($800) compared to many U.S. trading partners (Canada's *de minimus*, for example, is C$20, approximately $15, recently).
- **Localization requirements**. Governments may use privacy or national security arguments as justifications to compel companies to conduct certain digital-trade-related activities within a country's borders such as manufacturing or data processing.
- **Cross-border data flow limitations**. Regulations limiting cross-border data flows and requiring local storage are a type of localization requirement that prohibits companies from exporting data outside a country. Governments may claim legitimate policy objectives such as protecting privacy or cybersecurity as justifications for data localization measures. These restrictions can pose barriers to companies whose transactions rely on the internet to serve customers abroad, manage global value chains, and operate more efficiently. Limiting the ability to move data across national lines may constrain the ability to use innovative technologies such as blockchain applications because cross-border data flows are needed to share and store data on a blockchain with global partners for supply chain tracking, trade finance, customs and border clearance, or other international transactions.

  According to a 2017 USITC report, U.S. firms cited data localization as the top policy measure impeding digital trade, and the number of data localization measures globally has doubled in the last six years.[14] One U.S. business group noted increased forced localization measures, citing examples in China, Colombia, the European Union (EU), Indonesia, South Korea, Russia, and Vietnam,[15] while another highlighted barriers to cloud services in Indonesia, Russia, and Vietnam.[16]
- **Intellectual property rights (IPR) infringement.** IPR infringement includes copyright piracy, counterfeiting of trademarks, circumvention of technological protection measures (TPMs), cyber-theft of trade secrets, and trademark infringement related to domain names. By its nature, IPR infringement is difficult to quantify, and doing so in the digital environment is all the more challenging given that, for example, "infringing files are traded online and websites offering counterfeits are launched and accessed, countless

[13] During the 2017 WTO Ministerial meeting, some African countries suggested discontinuing the current moratorium. Communication from the African Group, *Draft Ministerial Decision on Electronic Commerce*, November 20, 2017.

[14] USITC, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, August 2017, https://www.usitc.gov/publications/332/pub4716.pdf.

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

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

times each day."[17] According to USTR, online sales of pirated and counterfeit goods reportedly could exceed the volume of sales "through traditional channels such as street vendors and other physical markets." A 2016 International Chamber of Commerce (ICC) study estimated the value of digitally pirated music, movies, and software (not actual losses) as $213 billion in 2013 to potentially $384-$856 billion in 2022.[18]

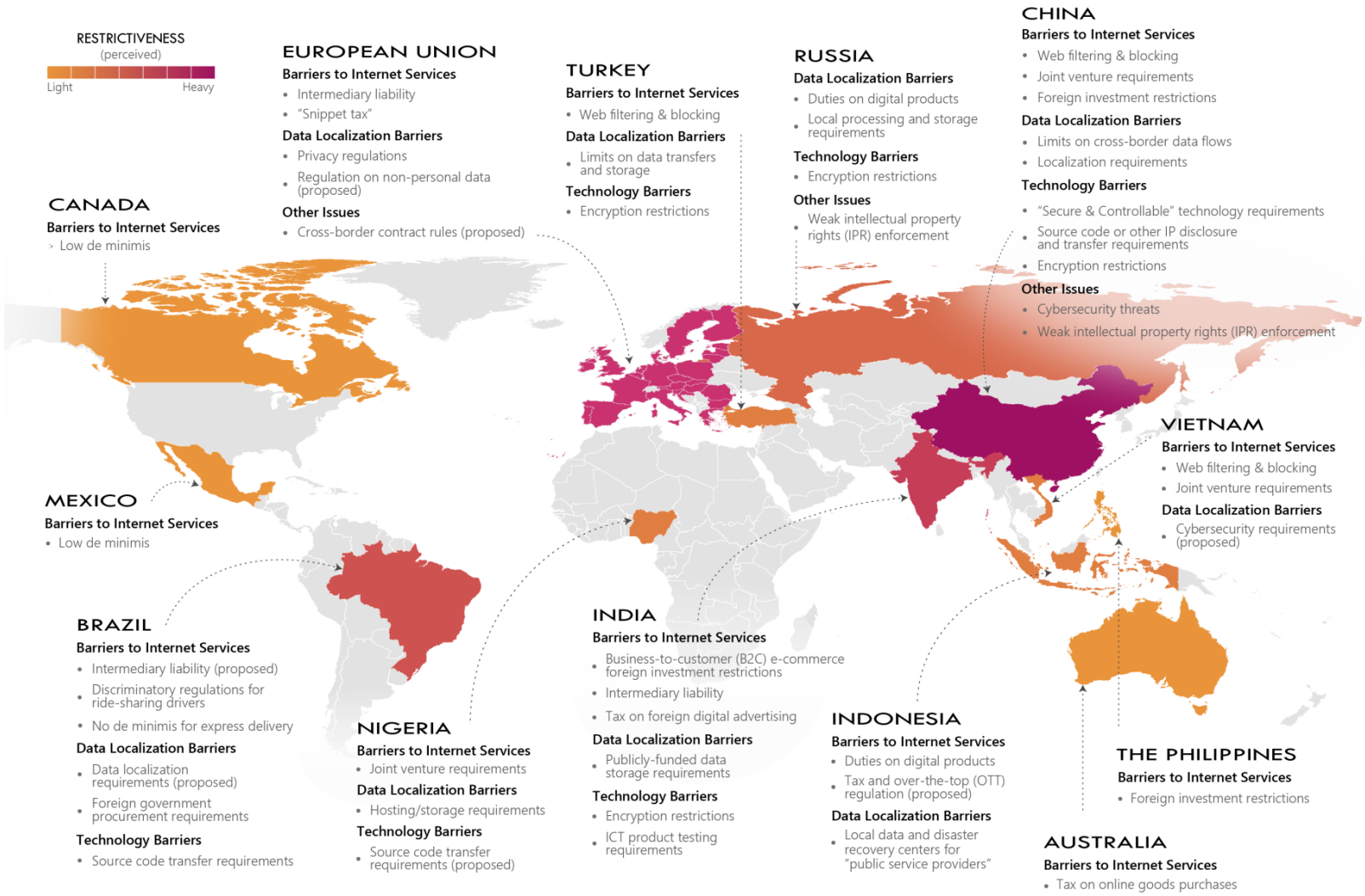
- **Discriminatory, unique standards or burdensome testing**. Local or national standards that deviate significantly from recognized international standards may limit interoperability or increase costs, and redundant testing or local registration requirements may make it difficult to enter or deter firms from entering a particular market.
- **Filtering or blocking of online content**. Governments may seek strict control over digital data within their borders, such as what information people can access online, and how information is shared inside and outside its borders.
- **Restrictions on electronic payment systems**. Lack of access to online payment options by foreign providers restricts the ability for companies or customers to sell and purchase online.
- **Cybersecurity concerns** including:
  - **Cyber-theft of U.S. trade secrets**. Cyber-attacks in general are deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. According to the White House Council of Economic Advisers, malicious cyberactivity (i.e., business disruption, theft of proprietary information) cost the U.S. economy up to $109 billion in 2016.[19]
  - **Forced technology transfer or restrictive cyber-security laws**. Requiring a firm to transfer its proprietary technology or reveal its source code in order to gain market access may deter firms from entering a market or undermine their competitiveness.
  - **Restrictions on cryptography and the use of encryption**. Limiting the ability to encrypt data, or controlling the type of encryption used, may expose a company to cybersecurity risks, serving as a deterrent to market entry.

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

[18] USTR, 2017 Special 301 Report, April 2017; Frontier Economics, The Economic Impacts of Counterfeiting and Piracy, report commissioned by Business Action to Stop Counterfeiting and Piracy (BASCAP) of the International Chamber of Commerce (ICC), June 2017.

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

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



Source: CRS analysis based on U.S. Trade Representative, 2018 National Trade Estimate Report on Foreign Trade Barriers, available at https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

Notes: *This map may be used in other CRS products. This map is illustrative of prominent digital trade barriers and not meant to be an exhaustive list

Digital Trade Rules

No single set of international rules or disciplines governs digital trade issues. Given the stalemate in the WTO negotiations, multilateral trade agreements have not kept pace with the complexities of the digital economy and digital trade is treated unevenly in existing WTO agreements. The rules are evolving piecemeal as governments experiment with different approaches and consider diverse policy priorities and objectives. These diverse country-specific rules may not always align with U.S. goals or policies.

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. The lack of globally accepted rules and standards for digital trade means that individual economies around the world are creating their own rules and regulations impacting market access. For my testimony, I will focus on two large economies and how they are shaping international rules. China and the EU each use their market size to set terms that other trading partners, and U.S. companies seeking to do business in their markets, must follow.

China

With a fundamentally distinct approach to the Internet compared to Western countries, China presents a number of significant opportunities and challenges for the United States in digital trade. In 2008, China overtook the United States as the world's largest Internet user (at 299 million versus 225 million users).[20] As of April 2017, China had 717.3 million Internet users.[21] China is the world's largest market for retail E-commerce, making it an attractive market for U.S. businesses. In 2016, China's E-commerce sales were estimated at $911 billion compared to $384 billion for the United States. [22] However, China's policies and actions have limited the ability of U.S. firms to enter or compete in the Chinese market.

Internet Sovereignty

The Chinese government has sought to advance its views on how the Internet should be expanded to promote trade, but also to set guidelines and standards over the rights of governments to regulate and control the Internet, a concept it has termed "Internet Sovereignty."[23] The Chinese government appears to have first advanced a policy of "Internet Sovereignty" around June 2010, stating:

> "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security."[24]

[20] *Internet World Stats*, 2017, available at http://www.Internetworldstats.com/stats3.htm.

[21] Newzoo, *Top 50 Countries by Smartphone Users and Penetration*, 2017, available at https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/.

[22] eMarketer, *Worldwide retail eCommerce Sales: iMarketer's Updated Estimates and Forecast Through 2019*, 2016, available at https://www.emarketer.com/public_media/docs/eMarketer_eTailWest2016_Worldwide_ECommerce_Report.pdf.

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

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

In December 2016, the Chinese government issued a National Cybersecurity Strategy, that emphasized China's view of cyber sovereignty and its right to promulgate policies in line with its own priorities without other countries interfering in its cyberspace.[25]

China has erected what is termed by some as the "Great Firewall," censoring and limiting what websites and information is available through the Internet in China. A 2018 report by the USTR cited a number of Internet-related barriers, noting that China currently blocks 12 of the top 30 global sites and up to 3,000 sites in total, limiting U.S. companies' access to Chinese customers.[26] A change to China's internet filters also blocks virtual private network (or VPN) access to sites beyond the Great Firewall. VPNs have been used by individuals and businesses in China to access websites like Facebook or data (e.g., information from foreign subsidiaries or partners) outside of China.[27]

China's Internet sovereignty initiative represents its assertion that the government has the right to limit information and fully control the Internet within China while some see it as further evidence of a more assertive Chinese foreign policy. Other critics of China's Internet Sovereignty policy view it as an attempt by the government to limit market access by foreign Internet, digital, and high technology firms in China, in order to boost Chinese firms and reduce China's dependence on foreign technology.

Cybersecurity Law

On November 7, 2016, the Chinese government passed a new Cybersecurity Law, that came into effect June 1, 2017. The American Chamber of Commerce in China (AmCham China) noted in particular the law's broad restrictions on cross-border data flows, and warned that they would "create barriers to Chinese as well as foreign companies operating in industries where data needs to be shared internationally."[28] The law's data localization requirements create a barrier to companies that want to use U.S. cloud-based services to access or better serve Chinese customers, share information with headquarters or subsidiaries abroad, or use innovative technologies such as blockchain[29] that depend on free flow of information.

A 2017 USTR report cited "significant declines in commercial sales of foreign ICT products and services in China," as evidence that China continued to maintain "mercantilist policies under the guise of cybersecurity."[30] Some analysts have expressed concerns that one of the main goals of the new cybersecurity law is to promote the development of indigenous technologies and impose restrictions on foreign firms. For example, the law 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."[31] The new law mandates reviews by the Cyberspace Administration of China (CAC) on foreign and domestic technology suppliers to ensure that their technology is "secure and controllable."

---

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

[26] USTR, *2018 National Trade Estimate Report on Foreign Trade Barriers*, March 2018.

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

[28] AmCham China, *AmCham China Statement on Cybersecurity Law*, November 7, 2017, at https://www.amchamchina.org/about/press-center/amcham-statement/amcham-china-statement-on-cybersecurity-law.

[29] Blockchain is a distributed record-keeping system (each user can keep a copy of the records) that provides for auditable transactions and secures those transactions with encryption. Using blockchain, each transaction is traceable to a user, each set of transactions is verifiable, and the data in the blockchain cannot be edited without each user's knowledge.

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

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

The CAC can also refuse to certify a product for unspecified risks to national security.[32] The term "secure and controllable" is another ambiguous term that has not been fully defined by Chinese authorities, raising concerns that it could be used as a process either to lock out foreign technology firms in China or force them to transfer technology and share proprietary information, such as source code (to demonstrate that there are no vulnerabilities that hackers can exploit), with Chinese regulators or partners.

IPR Theft

China is considered by most analysts to be the largest source of global theft of IP and a major source of cyber theft of U.S. trade secrets, including by government entities, deterring some U.S. firms from entering the Chinese market and potentially limiting the profitability of those that do. American firms cite the lack of effective and consistent protection and enforcement in China of U.S. IPR as one of the largest challenges they face in doing business in China.[33] Although China has improved its IPR protection regime over the past few years, many U.S. industry officials view piracy rates in China as unacceptably high. A 2017 survey by the U.S.-China Business Council found that 94% of respondents said they were concerned about IPR in China.[34]

Technology transfer requirements, whether formal through regulations limiting foreign investment or requiring joint ventures, or informal by applying pressure on companies seeking to do business in China, are a major complaint of U.S. firms seeking to protect their proprietary information. A 2018 USTR Section 301 investigation into Chinese laws, policies, practices, and actions that may harm American IPR, innovation, or technology development concluded that China (1) uses joint venture requirements, foreign investment restrictions, and administrative review and licensing processes to force or pressure technology transfers from American companies; (2) uses discriminatory licensing processes to transfer technologies from U.S. companies to Chinese companies; (3) directs and facilitates investments and acquisitions that generate large-scale technology transfer; and (4) conducts and supports cyber intrusions into U.S. computer networks to gain access to valuable business information. The USTR estimated that such policies cost the U.S. economy at least $50 billion annually.[35]

China's Influence on Other Countries

China's FTAs have limited commitments on digital trade. For example, the Australia-China FTA contains a chapter on electronic commerce, with provisions relating to the prohibition of customs duties on electronic transmissions, regulatory transparency, and consumer protection among others. However, it is not enforceable through the agreement's dispute settlement procedures, potentially limiting its effectiveness.

Many analysts argue that China's policies are setting protectionist precedents globally, limiting market access to U.S. or other foreign firms and potentially splintering or fragmenting the Internet. Other countries have sought to imitate China's policies by requiring local data storage and limiting cross-border data flows, filtering and censoring online content, or requiring access to source code in the name of

[32] 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.

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

[34] Ibid.

[35] The USTR investigation followed a presidential memorandum and was conducted under Section 301 of the Trade Act of 1974. For more information on the Section 301 investigation, see CRS In Focus IF10708, *Enforcing U.S. Trade Laws: Section 301 and China*, by Wayne M. Morrison.

national security or cybersecurity. As noted above, Russia and Vietnam have used cybersecurity as a rationale for laws that require local data storage.

European Union

While the United States and the EU share broad objectives for an open and rules-based international trading system, particular differences in policies may have ramifications on digital flows and international trade with significant economic consequences given the size of the trading relationship. The transatlantic economy accounts for half of the global gross domestic product by value,[36] and cross-border data flows between the United States and EU are the highest in the world. As of 2016, the United States and EU traded $2.7 billion a day worth of goods and services, and the annual digital services trade between the two regions is approximately $260 billion.[37] The two partners' varying approaches to digital trade, privacy, and national security, have, at times, threatened to disrupt U.S.-EU data flows.

Data Privacy and Protection

The United States and EU have different legal approaches to information privacy that extends into the digital world. The EU considers the privacy of communications and the protection of personal data to be fundamental rights, which are codified in EU law. Europe's history with fascist and communist regimes informs the EU's views on data protection and contributes to the demand for strict data privacy controls. The EU regards U.S. data protection safeguards as inadequate; this has complicated the conclusion of U.S.-EU information-sharing agreements and raised concerns about U.S.-EU data flows that many U.S. firms depend on to access EU customers and operate efficiently.

After extensive negotiations, the EU-U.S. Privacy Shield became operational in August 2016, providing a framework to provide U.S. and EU companies a mechanism to comply with data protection requirements when transferring personal data between the EU and the United States.[38] Under the Privacy Shield program, U.S. companies can voluntarily self-certify compliance with requirements such as robust data processing obligations. The agreement includes obligations on the U.S. government to proactively monitor and enforce compliance by U.S. firms, establish an ombudsman in the U.S. State Department, and set specific safeguards and limitations on surveillance. The Privacy Shield also involves an annual joint review by the United States and the EU, the first of which was conducted in September 2017.[39] The United States and Switzerland also agreed to the Swiss-U.S. Privacy Shield, which will be "comparable" to the U.S.-EU agreement.[40]

Subsequent to the signing of Privacy Shield, the EU agreed on a new General Data Protection Regulation (GDPR), which became applicable on May 25, 2018. The GDPR established a single set of rules for protection of personal data throughout the EU that seeks both to strengthen individual fundamental rights in the digital age and facilitate business by ensuring more consistent implementation of the rules EU-

[36] http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/.

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

[38] For more information on the Privacy Shield, see CRS Report R44257, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, by Martin A. Weiss and Kristin Archickand https://www.privacyshield.gov/Program-Overview.

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

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

wide. The GDPR is seen by some as the most comprehensive privacy regulation impacting digital trade globally and potentially precedent-setting for how businesses conduct themselves in regards to personal data.

The GDPR identifies what is a legitimate basis for data processing and sets common rules regarding data retention, storage limitation, and record keeping. Processing certain sensitive personal data is generally prohibited. Stronger and new data protection requirements grant individuals the right to:

- Receive clear and understandable information about who is processing one's personal data and why;
- Consent affirmatively to any data processing;
- Access any personal data collected;
- Rectify inaccurate personal data;
- Erase one's personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data (the "right to be forgotten");
- Restrict or object to certain processing of one's data;
- Be notified without "undue delay" of a data breach if there is a high risk of harm to the data subject; and
- Require the transmission of one's data to another controller (data portability).

The potential high penalties for non-compliance have attracted significant attention since a company or organization can be fined up to 4% of its annual global turnover or €20 million (whichever is greater). Fines are to be assessed by the national supervisory authority (a Data Protection Authority, or DPA) in each member state and subject to appeal in national courts. Some stakeholders are concerned about possible uneven enforcement by EU Member States. The GDPR also requires some companies to hire data protection officers.[41]

U.S. firms have voiced several concerns about the GDPR, including how it is implemented and the scale of potential fines. Some companies are concerned about the need to construct a compliance bureaucracy and possible high costs for adhering to the GDPR's requirements. While large firms have the resources to hire consultants and lawyers, it may be harder and costlier for SMEs to comply, possibly deterring them from entering the EU market and creating a de facto trade barrier. Reports suggest that some SMEs have opted to exit or limit offerings or services to the EU market given the complexities of complying with the GDPR, possibly limiting competition and customer choice.

Another issue is that the GDPR right to erasure could clash with freedom of information, and, for U.S. firms, with the First Amendment. The GDPR includes exceptions and recognizes the need to balance the right to personal data protection with freedom of expression, but advocates worry that Internet companies may be quick to grant erasure requests to avoid possible legal challenges, which, over time, could erode information online. Many Internet companies share such concerns, viewing the GDPR erasure provisions as pitting the "right to be forgotten" against the "right to know."

Under the GDPR, the U.S.-EU Privacy Shield will continue to serve as a mechanism for participating U.S. and EU companies that meet EU data protection requirements. However, Privacy Shield is not a GDPR compliance mechanism and participation by a company in Privacy Shield does not guarantee full GDPR compliance.

[41] For more information on the GDPR, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick, and https://www.eugdpr.org/.

Some observers and government officials worry about the potential negative impact of the GDPR on innovation, including the use of blockchain or artificial intelligence, and on the WHOIS database (managed by the Internet Corporation for Assigned Names and Numbers, or ICANN) that stores information about the registrants and operators of websites.[42] Law enforcement and cybersecurity researchers often use WHOIS to identify hackers and malicious Internet domains. WHOIS data could now be protected under the GDPR, and some worry this will undercut WHOIS as an effective cybersecurity tool. ICANN has begun filing legal action in EU countries restricting access under GDPR.[43]

In addition to GDPR, the EU's draft ePrivacy Regulation has also raised concerns among companies and industry groups who see the current proposal bringing digital communications under the same rules as traditional telecommunications as too onerous and restrictive.[44] While some advocate the regulation as needed consumer protection to ensure the privacy of electronic communications, others voice concern that it may hinder innovation gains of machine-to-machine communication or Internet of Things (IoT) applications. As GDPR went through multiple drafts being finalized, the ePrivacy Regulation may be further refined as it goes through the EU legislative process.

EU Influence on Other Countries

In its free trade negotiations with other countries, the EU has few hard commitments in regard to digital trade apart from prohibiting customs duties on electronic deliveries; instead it emphasizes regulatory dialogue. Cross-border data flows are not protected under EU FTAs and the EU did not want to include the topic in the U.S.-EU Transatlantic Trade and Investment Partnership (TTIP) negotiations under the Obama Administration. For example, the Comprehensive Economic and Trade Agreement (CETA) between the EU and Canada, the most recent EU FTA that has entered into force, establishes a dialogue on multiple digital trade issues and requires parties to have measures to protect personal information of users but does not explicitly require a GDPR-like regime.[45] CETA does not mention cross-border data flows nor are data flows addressed in the EU-Japan FTA, which has yet to be ratified by the EU, although the parties agree to discuss the issue in the future.[46]

As no multilateral rules on cross-border data flows or data privacy exist, some experts contend that the GDPR may effectively set new global data privacy standards as companies and organizations strive for compliance to avoid being shut out of the EU market. Some companies may determine that it is easier to comply with EU regulations globally rather than implement changes for only the EU market. "In the absence of another approach, it's easier for other markets to follow what Europe has done," said Dean C. Garfield, president of the Information Technology Industry Council.[47]

Regarding privacy, European Commissioner for Justice, Consumers and Gender Equality, Vera Jourova, has stated, "We want to set the global standard."[48] Some countries are adopting GDPR-like regimes to

[42] ICANN, "Data Protection/Privacy Update: Seeking Additional Clarity from Article 29," May 10, 2018.

[43] ICANN, "ICANN Files Legal Action in Germany to Preserve WHOIS Data," May 25, 2018, https://www.icann.org/news/announcement-2018-05-25-en.

[44] For more information on the ePrivacy Regulation, see https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[45] EU-Canada Comprehensive Economic and Trade Agreement (CETA) Chapter 16 Electronic Commerce, http://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/.

[46] Proposal for a Council Decision on the conclusion of the Economic Partnership Agreement between the European Union and Japan, Article 8.87, April 18, 2018.

[47] Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *New York Times*, May 24, 2018.

[48] Mark Scott and Laurens Cerulus, "Europe's new data protection rules export privacy standards worldwide," *PolitocPro*, (continued...)

ensure that the EU allows for cross-border data flows between the parties,[49] to facilitate domestic companies doing business in the EU, or as a short-cut to establishing a domestic privacy framework.[50] Countries such as Brazil, Japan, and South Korea have explicitly sought advice from the EU for their own data protection laws while others aim to update their rules to meet EU levels. U.S. privacy advocates have encouraged U.S. firms to adopt changes made to comply with the GDPR in the United States as well, viewing the changes as advancing consumer protection. Privacy and consumer advocates have also voiced support for the establishment of a comprehensive U.S. privacy policy similar to the GDPR.

Establishing International Digital Trade Rules

Some view China and the EU as seeking to impose their views and standards globally, using their large market size to guide international practices. These observers contend that the United States should proactively counter Chinese and EU efforts to move forward with new digital trade policies that may limit market access to U.S. firms. Some analysts suggest that the United States should focus attention on developing new digital trade rules and disciplines through ongoing and future bilateral and plurilateral trade negotiations in line with U.S. policy and priorities.

Trade Promotion Authority

The growth in trade barriers has raised the prominence of digital trade on the trade agenda. Congress recognized the importance of digital trade and removing related barriers in the negotiating objectives of its most recent grant of Trade Promotion Authority (TPA), the Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (P.L. 114-26), signed into law in June 2015.[51] TPA 2015 objectives related to digital trade direct the Administration to negotiate agreements that:

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

Negotiating Forums

Some see a risk to U.S. market access and influence if the Unites States does not actively seek to establish new international trade rules while large economies such as China and the EU push forward with policies reflecting their vision of the Internet and digital trade.

The proposed Trans-Pacific Partnership (TPP), negotiated by the United States during the Obama Administration, was seen by some as having the most comprehensive digital trade commitments of any

(...continued)

February 6, 2018.

[49] Countries may seek "adequacy" decisions by the EU to allow for cross-border data flows. The U.S.-EU Privacy Shield serves as an alternative to a full adequacy decision by the EU.

[50] Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *New York Times*, May 24, 2018.

[51] 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.

FTA to date. The TPP aimed to promote digital trade, promote the free flow of information, and ensure an open internet.[52] After President Trump withdrew the United States from the TPP, the eleven remaining countries negotiated and signed a revised agreement without the United States, which is now in the ratification process. The revised TPP, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), made modifications to select IPR and investment commitments but largely retained the provisions of the original agreement, including on digital trade.[152] For example, the CPTPP requires parties to have a legal framework to protect personal information. Privacy frameworks such as the EU's GDPR and the international Asia-Pacific Economic Cooperation (APEC) Privacy Framework and Cross Border Privacy Rules (CBPRs) (to which the United States belongs) would be permitted under the CPTPP provisions.[53] Some view the TPP as a lost opportunity for the United States to set global rules and best practices on digital trade.

New and ongoing bilateral and plurilateral negotiations present opportunities for the United States to establish rules and disciplines on digital trade.

- **North American Free Trade Agreement (NAFTA).** Like the Uruguay Round agreements, which created the WTO, NAFTA also entered into force in the 1990's, predating mass usage of the internet. The ongoing NAFTA renegotiations provide an opportunity to address digital trade.[54] Some have suggested the TPP text could provide a starting point while others contend that the revised NAFTA should go beyond those commitments such as by specifying a *de minimus* standard. Canada and Mexico may soon be party to similar commitments through their participation in the CPTPP.
- **E-commerce Plurilateral**. In December 2017, on the sidelines of the 11th WTO Ministerial Conference in Buenos Aires, Argentina, a group of over 70 WTO members, including the United States, agreed to "initiate exploratory work together toward future WTO negotiations on trade related aspects of electronic commerce."[131] USTR supported the movement toward plurilateral efforts stating, "the United States is pleased to work with willing Members on e-commerce, scientific standards for agricultural products, and the challenges of unfair trade practices that distort world markets."[132] Members are currently discussing which aspects of digital trade they will address in any negotiations. The United States put forth its objectives, including market access, data flows, fair treatment of digital products, protection of intellectual property and digital security measures, and intermediary liability, among others.[133]
- The **G-20, OECD**, **APEC**, and bilateral forums all provide international venues outside of trade negotiations that can be used to establish high-level, nonbinding best practices and principles and align expectations on digital trade.
- **Technology Transfer.** In May 2018, the United States, the EU, and Japan agreed to "deepen cooperation and exchange of information, including with other like-minded partners, to find effective means to address trade-distorting policies of third countries, including harmful forced technology transfer policies and practices, and where appropriate, to pursue dispute settlement proceedings at the WTO."[55] The three agreed to establish and share best practices and work together to end technology transfer policies by other countries.

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

[53] For more information on the APEC Privacy Framework, see https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

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

[55] U.S. Trade Representative Press Release, "Joint Statement on Trilateral Meeting of the Trade Ministers of the United States, (continued...)

(...continued)
Japan, and the European Union," May 2018.