PIIE PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS

POLICY BRIEF

19-14 Global E-Commerce Talks Stumble on Data Issues, Privacy, and More

Gary Clyde Hufbauer and Zhiyao (Lucy) Lu

October 2019

Gary Clyde Hufbauer is nonresident senior fellow at the Peterson Institute for International Economics. **Zhiyao (Lucy) Lu** was a research analyst at the Peterson Institute for International Economics from March 2016 to February 2019. Views expressed here are solely their own.

Since the collapse of the Doha Round of multilateral trade negotiations a decade ago, efforts to reduce trade barriers on a worldwide basis have been pitiful. Nevertheless, in early 2019, off the radar screen of media attention, several important members of the World Trade Organization (WTO)—including the United States, European Union, and China—submitted noteworthy proposals in a realm of international commerce that has received scant attention from the public: what is known as e-commerce or digital trade.

At a time of explosive growth in commercial activity over the internet and social media, these new modes of international trade have evolved faster than rules to govern them. For example, when a European consumer searches on Amazon.com to buy a laptop, Amazon might store the consumer's searching keywords and browsing history on its local European server, so that the company can offer personalized advertisements, or it might store that data at the headquarters in Seattle. What rights does that consumer have to the use and location of that data? What control should individual citizens or countries retain over this sort of commerce, and what powers should countries have to raise or avoid taxes? Who will control fraudulent or deceptive commercial practices or the standardization of electronic signatures?

Amid general recognition that trading rules put forward by the WTO have hardly begun to deal with these issues, some 76 WTO member states (the 28 EU members and 48 other WTO countries) launched plurilateral negotiations among themselves to define acceptable e-commerce practices (often, but not always, a synonym for digital trade) in January 2019.[1] The United States has joined about a dozen WTO members, including China, the European Union, Japan, Singapore, and Brazil, to submit proposals. In the June 2019 meeting in Japan, the Group of Twenty (G-20) leaders launched the "Osaka Track" to formulate rules on trade-related aspects of e-commerce in the WTO.[2] G-20 leaders seek to "achieve a high standard agreement with the participation of as many WTO Members as possible." If it does anything, the "Osaka Track" essentially provides a boost to the WTO plurilateral negotiations, the only game in town.

Countries agree on less controversial subjects like banning unsolicited commercial electronic messages, ensuring the validity of electronic contracts, protecting online consumers from fraudulent or deceptive commercial practices, and recognizing electronic authorization and electronic signatures. But the three leading members—China, the European Union, and the United States—have big differences in their approaches to more challenging issues: data flows, data localization, privacy invasions by data collectors, transfer of source code, imposition of customs duties and internet taxes, and internet censorship (table 1).[3]

---

1. "76 WTO partners launch talks on e-commerce," European Commission, January 25, 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974 (accessed on June 25, 2019).

2. For the "Osaka Track," see "Osaka Declaration on Digital Economy," https://g20.org/pdf/special_event/en/special_event_01.pdf (accessed on July 3, 2019).

3. Since the US proposal is not publicly available, our summary of US positions is based on *Inside US Trade* reports as well as the United States-Mexico-Canada Agreement (USMCA) Chapter 19 on Digital Trade, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf (accessed on September 29, 2019). For China's proposal on WTO e-commerce negotiations, see "Joint Statement on Electronic Commerce: Communication from China," INF/ECOM/19, World Trade Organization, April 24, 2019, https://docs.wto.org/dol2fe/Pages/FE_Search/

Table 1
US, EU, and Chinese positions on contentious e-commerce issues

Issue	United States	European Union	China
Data flows	Free data flows with exceptions	Free data flows with exceptions	Skeptical about free data flows
Data localization	Ban data localization	Ban data localization	Skeptical about prohibition of data localization
Privacy	Restrictions should only be necessary and proportionate to privacy risks presented	Restrictive measures could be applied to protect privacy	Restrictive measures could be applied to protect privacy and ensure security
Source code	Ban forced transfer of source code with exceptions	Ban forced transfer of source code with exceptions	Not addressed in proposal, but is not expected to make commitments
Customs duties	Promote zero customs duties	Promote zero customs duties	Promote zero customs duties until the next WTO ministerial conference
Internet taxes	Opposes internet taxes	Advocates internet taxes	Position unknown
Open internet access	Favored with exceptions	Favored with exceptions	Strong state control

Reconciling the positions of China, the European Union, and the United States will be essential to the success of e-commerce talks. This Policy Brief summarizes Chinese, US, and EU positions on key questions to gauge the difficulty of reaching a consensus among the three. Their differing viewpoints lead to the conclusion that the outlook is pessimistic. The number of participating countries currently involved in the WTO negotiations must be sharply reduced to reach a high-standard robust agreement.

As an alternative, the scope of WTO e-commerce negotiations needs to be sharply narrowed to exclude difficult issues so that participating WTO members can conclude a basic e-commerce pact. It is worth noting that a low-ambition accord to establish basic digital norms on matters such as banning unsolicited commercial electronic messages, ensuring the validity of electronic contracts, protecting online consumers from fraudulent or deceptive commercial practices, and recognizing electronic authorization and electronic signatures would still be valuable and, more importantly, would revitalize the WTO negotiating arm, which managed to enact a Trade Facilitation Agreement in 2017 but has otherwise been paralyzed for years.

WTO E-COMMERCE NEGOTIATIONS: BACKGROUND

Digital flows include everything from entertaining movies and music to instruction in mathematics and engineering to performance data on refineries, factories, and offices; examples include Netflix movies, Spotify music, and massive open online courses. More obscure but equally important are the enormous daily data flows between the global subsidiaries of multinational corporations—ExxonMobil, GE, Caterpillar, Apple, Microsoft, JPMorgan Chase, and many others. E-commerce is usually defined more narrowly to cover just transactions between sellers and buyers, accompanied by payment using an internet platform. It remains to be seen what definition is agreed in the WTO e-commerce negotiations.[4]

DDFDocuments/253560/t/INF/ECOM/19.docx (accessed on June 25, 2019). For the EU proposal, see "Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce," INF/ECOM/22, World Trade Organization, April 26, 2019, https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf (accessed on August 29, 2019).

4. In its Work Programme on Electronic Commerce, the WTO defines e-commerce as "the production, distribution, marketing, sale or delivery of goods and services by electronic means." See WT/L/274, September 30, 1998, www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm (accessed on September 23, 2019). The OECD defines an electronic transaction as "the sale or purchase of

In any event, international digital flows have expanded rapidly in recent years, making a substantial contribution to the global economy. The McKinsey Global Institute (2016) estimated that global data flows were 45 times larger in 2014 than in 2005. Digitalization lowers trade costs and improves productivity through better connectivity. Longmei Zhang and Sally Chen (2016) at the International Monetary Fund found that a 1 percentage point increase in the overall digitalization of an economy is correlated with an increase of 0.3 percentage point of GDP growth with a two-year lag. The United States International Trade Commission (USITC 2014) estimated with a computable general equilibrium model that digital trade—defined by the USITC as US domestic commerce and international trade facilitated by or conducted via the internet—raised US real GDP by 3.4 to 4.8 percent compared with the baseline scenario in 2011, through the combined economywide effects of enhanced productivity and lower trade costs. Removing foreign barriers to digital trade in digitally intensive industries would have raised US GDP by 0.1 to 0.3 percent in 2011. AlphaBeta defines digital trade as the production, distribution, marketing, sale, or delivery of goods and services—domestically and abroad—supported by cross-border data flows. According to AlphaBeta, digital trade contributed $466 billion to China's GDP in 2017, and the contribution could reach $5.5 trillion by 2030.[5] Paul Hofheinz and Michael Mandel (2015) found that digital density measured as per capita data usage correlates positively with investment in intangible assets. They estimated that if digital density in six European countries—Sweden, the United Kingdom, France, Germany, Spain, and Italy—could rise to the US level, their level of intangible investments would rise by €459 billion.

Yet despite its increasing importance and promising gains, no comprehensive and standalone WTO agreement governs e-commerce, or digital trade. Existing WTO agreements—the General Agreement on Trade in Services, the Information Technology Agreement, and the Agreement on Trade-Related Aspects of Intellectual Property Rights—cover certain aspects of e-commerce.[6] However, they leave giant gaps, allowing countries to implement barriers such as data localization requirements and digital taxes. Amid lethargic growth in conventional trade and growing protectionism, e-commerce could continue to serve as a strong source of economic growth.[7] At the same time, balance needs to be achieved between this new and rapidly expanding form of commerce and demands for personal privacy and national security.

Reflecting these considerations, in January 2019 the European Union and 48 other WTO members commenced WTO negotiations on electronic commerce, seeking to "achieve a high standard outcome" and to further "enhance the benefits of electronic commerce for businesses, consumers, and the global economy."[8]

CONTENTIOUS E-COMMERCE ISSUES: US, EU, AND CHINESE POSITIONS

Data Flows

In the digital era, an increasing share of production and trade takes place over the internet, while the internet has transformed traditional business models. The strong growth of data-driven business models depends on the ability of companies to store, move, and use digital information efficiently, especially across borders.[9] However, concerns arise about how vast troves of data might be transformed and used. Accordingly, governments have imposed regulations to govern data flows, both within the country and across borders.[10]

The Chinese proposal in WTO e-commerce talks does not explicitly address the topic, but Beijing is skeptical about free cross-border data flows. It argues that "more exploratory discussions are needed before bringing such issues [data flow, data storage] to the WTO negotiation" and contends that data flow rules should reflect the precondition of security.

goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders." See Electronic Commerce, Glossary of Statistical Terms, OECD Statistics Portal, https://stats.oecd.org/glossary/detail.asp?ID=4721 (accessed on September 23, 2019). The OECD definition covers only the *ordering* of products, which is much narrower than the WTO definition.

5. See "The Data Opportunity: The promise of digital trade for China," AlphaBeta, www.alphabeta.com/our-research/the-data-opportunity-the-promise-of-digital-trade-for-china/ (accessed on August 29, 2019), and "Report: China becoming digital trade leader," *China Daily*, April 9, 2019, www.chinadaily.com.cn/a/201904/09/WS5cac3974a3104842260b52e3.html (accessed on August 29, 2019).

6. See "Digital Trade," Congressional Research Service, March 29, 2019, https://crsreports.congress.gov/product/pdf/IF/IF10770 (accessed on July 3, 2019).

7. See Gary Clyde Hufbauer and Zhiyao (Lucy) Lu, "Can Digital Flows Compensate for Lethargic Trade and Investment?" PIIE Trade and Investment Policy Watch, November 28, 2018.

8. See "Joint Statement on Electronic Commerce," WT/L/1056, World Trade Organization, January 25, 2019, https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf (accessed on September 29, 2019).

9. Relevant business models include cross-border shopping, within-firm flows of information, and provision of IT services that generate data.

10. For a detailed discussion on trade and data flows, see Casalini and González (2019).

It could be expected that China would make no commitments on free cross-border data flows. Article 37 of China's Cybersecurity Law, effective June 1, 2017, states that operators of critical information infrastructure (CII) must pass a security assessment by government agencies before transmitting personal and other important data overseas.[11] Violators will be punished by monetary fines and may lose their operating rights (Article 66). The Law defines CII as "important sectors including public telecommunication and information services, energy, transportation, water resource, finance, public services, e-government, as well as other CII that, if [they are] damaged, lose functionality, or experience data leakage, could seriously jeopardize national security, national economy, people's livelihood, and public interest" (Article 31). Obviously, this covers a broad scope. On July 11, 2017, the Cyberspace Administration of China (CAC) issued a draft Regulation on Critical Information Infrastructure Security Protection for public comment;[12] Article 18 of the document further defines the scope of CII under protection:

> (1) government agencies and companies in energy, finance, transportation, water resource, sanitation and healthcare, education, social security, environmental protection, and public utilities, etc.;
>
> (2) telecommunications networks, radio and television networks, the Internet and other information networks; companies that provide cloud computing, big data, and other large-scale public information network services;
>
> (3) research and production companies in national defense and science and technology, large-scale equipment, chemical products, food and drug, etc.;
>
> (4) radio stations, television stations, news agencies and other media agencies; and
>
> (5) other important companies.

In addition, the draft states that relevant government agencies will define CII by industries under their purview. Beijing has not yet released a final definition of CII or a list of companies deemed to be CII operators subject to the Cybersecurity Law's cross-border data flow restrictions, but vague language suggests the definition could be extensive.

Beyond designated CII operators that must store personal information and important data in China, draft regulations issued by the CAC in May and June 2019 also restrict cross-border flows of important data—data that, if leaked, could directly affect national security, economic security, social stability, public health and security—and personal information.[13] Hence, the potential scope of restrictions covers vast segments of cross-border data flows. Unless China is willing to dramatically narrow its existing and draft regulations, Beijing can make few if any commitments on cross-border data flows.

By contrast, both the United States and the European Union broadly favor free cross-border data flows, but with exceptions that could also be far-reaching. The United States allows restrictions to "achieve a legitimate public policy objective," such as measures that allow intelligence agencies to uncover terrorists and hackers. The United States commits to respecting two preconditions before applying data flow restrictions: (1) they should not be applied arbitrarily and (2) they should interrupt data flows as little as needed to achieve the objective. Very similar exceptions to the free flow of data are allowed in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (Article 14.11.3), an agreement the United States considered joining.[14] The European Union allows member states to design their own rules, in the interest of privacy, for the cross-border transfer of personal data.

Depending on the interpretation of exceptions, both US and EU restrictions on cross-border data flows could be extensive—in some circumstances as extensive as Chinese measures taken for security or privacy purposes. Preliminary soundings suggest that e-commerce talks will not yield rules that circumscribe national security or privacy concerns in determining which data flows can and cannot be transmitted

11. See "中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China]," National People's Congress, www.xinhuanet.com//politics/2016-11/07/c_1119867015.htm (accessed on June 24, 2019).

12. See "国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知 [Cyberspace Administration of China seeks comments on the Regulation of Critical Information Infrastructure Security Protection (version for comment)]," Cyberspace Administration of China, July 11, 2017, www.cac.gov.cn/2017-07/11/c_1121294220.htm (accessed on June 24, 2019).

13. On May 28, 2019, the CAC issued a draft Data Security Management Regulation for comment [数据安全管理办法（征求意见稿）], www.cac.gov.cn/2019-05/28/c_1124546022.htm (accessed on June 30, 2019). It requires network operators to "assess the potential security risks and seek approval from industry regulators before publishing, sharing, trading, or transferring important data overseas" (Article 28). On June 13, 2019, the CAC issued a draft Security Assessment on the Cross-border Transfer of Personal Information Out of China Regulation for comment [个人信息出境安全评估办法（征求意见稿）], www.cac.gov.cn/2019-06/13/c_1124613618.htm (accessed on June 30, 2019). It requires a security assessment by provincial cybersecurity agencies before transferring personal data overseas.

14. The precursor to the CPTPP was the Trans-Pacific Partnership, advocated by the Obama administration but never sent to Congress for ratification.

to foreign countries. Failure of agreement among China, the United States, and the European Union could also serve as a major impediment to future growth of the Internet of Things.

Data Localization

Data localization refers to the practice of requiring firms to locate their computing facilities in domestic territory as a precondition for conducting business in that territory. A growing volume of empirical research suggests that data localization provisions can inflict significant economic costs.[15] As with data flows, China is skeptical about measures that would limit policies promoting data localization for security and other purposes. In any event, the Chinese proposal does not address the question of server location by foreign-owned firms.

As a technical matter, the question of where data are stored could be differentiated from the permission to use and manage the data. Permission to use is the essence of restrictions on cross-border data flows. However, officials often believe that storing data in local servers is essential for effective control of cross-border data flows.

Contrary to China's position, the European Union and the United States would ban data localization as a condition for conducting business in a WTO member state.[16] The gap is wide between China's position (shared by many developing countries, such as Brazil, India, Indonesia, and Russia) and the EU/US position (shared by other advanced countries).

Privacy and Personal Data

The European Union and the United States have different interpretations and systems of privacy protection. The European Union views privacy and data protection as fundamental human rights and has a single set of privacy and data protection rules for all companies operating in the bloc through the General Data Protection Regulation (GDPR) (and its predecessor the Data Protection Directive).[17] In the United States, the Fourth Amendment protects individual privacy interests from *unreasonable* search and seizure by government officials. The US Supreme Court, starting with Mapp v. Ohio (1961), has decided many cases that define the line between reasonable and unreasonable searches and seizures. But the Fourth Amendment does not apply to private companies that collect and process personal data. Their actions are limited, if at all, by the prospect of civil litigation and money damages for the invasion of privacy.

Citizen privacy was a thorny issue in the erstwhile Transatlantic Trade and Investment Partnership (TTIP) negotiations between US tech giants and intelligence agencies, on the one hand, and EU privacy advocates on the other.

As with data flows, China is skeptical about measures that would limit policies promoting data localization for security and other purposes.

The European Union values privacy more, arguing that member states can implement measures—such as restrictions on cross-border flows of personal data—to protect privacy. By contrast, the United States places a higher value on free cross-border data flows and asks WTO members to ensure that any restrictions are "necessary and proportionate to the risks presented."

In an attempt to resolve differences, the two sides signed the Privacy Shield Pact on July 12, 2016, an auxiliary pact to the broader TTIP negotiations.[18] US firms operating in the European Union that self-certify their adherence to the Privacy Shield must also implement US Department of Commerce guidelines, or secure the agreement of individual EU citizens, before transferring personal data from the European Union to the United States.[19] Separate from the Privacy Shield Pact, the EU General Data Protection Regulation was issued in April 2016 and took effect in May 2018.[20] Facebook is now trying to limit the scope of the GDPR to EU users only, not the 1.8 billion users living outside the bloc. Currently users outside the United States and Canada, including those residing in Europe, Asia, and other regions, sign terms

15. Cory (2017) reviews several studies that assess the economic cost of data localization policies.

16. For the US position, see Article 19.12 on "Location of Computing Facilities" in the United States-Mexico-Canada Agreement (USMCA). For the EU position, see "2.7 Cross-Border Data Flows" in the EU proposal on WTO e-commerce negotiations.

17. The Data Protection Directive refers to "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed on June 29, 2019).

18. TTIP negotiations later fell apart.

19. For a detailed discussion of the US-EU Privacy Shield Pact, see Hufbauer and Jung (2016).

20. The GDPR regulates "the processing by an individual, a company or an organization of personal data relating to individuals in the EU." Companies doing business in the bloc have to (a) notify the public of any data breach; (b) give individuals the right to be forgotten; (c) assess the privacy impact of certain products, such as online marketing; and (d) build privacy into all products. See Hufbauer and Jung (2016).

of service with Facebook Ireland, registered in Ireland, not Facebook Inc., a US corporation. Facebook would like to make this portion of its users, except those in Europe, sign terms of contract with Facebook Inc. instead of Facebook Ireland, to minimize its exposure to the GDPR.[21] If applied worldwide, the GDPR would create a big compliance hassle for Facebook and kindred firms to require privacy contracts with all global users.

The US position in part reflects the commercial interest of giant internet firms (Amazon, Apple, Facebook, Google, etc.) in using personal characteristics to match advertisers with potential buyers.[22] For similar reasons, the United States promotes compatibility between different privacy regimes and among WTO members.

China seems to side with the European Union on privacy issues in its proposal, arguing that necessary and appropriate measures can be implemented to protect privacy. However, while the EU focus is personal rights, China's focus is security. On May 1, 2018, China's Information Security Technology—Personal Information Security Specification, modeled partly on the GDPR, went into effect.[23] Though it is only a privacy standard and does not have the legal power of a law, Article 8.7 specifies that cross-border transfer of personal information must undergo a security assessment by cybersecurity agencies and relevant departments under the State Council. The previously discussed draft regulation on cross-border transfer of personal information issued by the CAC in June 2019 seems to be a follow-up document on this specification.

Strong end-to-end encryption might allay some privacy concerns. However, the difficulty of encrypting multiparty platforms, such as Facebook, coupled with the economic hurdles to mass encryption mean that encryption could at best reconcile only part of the gap between US and EU approaches. The bigger gap concerns the permitted use that firms such as Facebook or Amazon make of personal data. Moreover, the 2016 encryption dispute between Apple and the Federal Bureau of Investigation indicates that strong encryption could create significant hurdles for law enforcement and intelligence agencies.[24] Given these obstacles, an agreement that reconciles differing national approaches to personal privacy seems elusive.

Transfer of Source Code

Source code for software is a set of human-readable instructions that a programmer writes when creating a program. It can be translated into machine language that is computer readable. Again, China does not address source code in its proposal but is not expected to make commitments, while the United States and the European Union broadly prohibit forced transfer of software source code as a precondition for conducting business in a foreign country.[25] The latter is also the position in the CPTPP.[26]

The United States and the European Union both have exceptions, but they differ. The United States advocates exceptions to comply with regulatory decisions without causing the owner to lose the trade secret status of its software. An example might be source code for financial transactions, required to be disclosed to the Treasury Department so that it can guard against money laundering or evasion of economic sanctions. The European Union lists three situations in which forced disclosure of source code is permitted: (1) to remedy a violation of competition law, (2) to protect and enforce intellectual property rights, and (3) to address security concerns.

21. See "Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law," Reuters, April 18, 2018, www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P (accessed on July 3, 2019).

22. Some politicians and scholars argue for a data sharing mandate to introduce more competition to break internet monopolies. See, for example, Biancotti and Ciocca (2019).

23. See 中华人民共和国国家标准 GB/T 35273-2017 信息安全技术 个人信息安全规范" [Information security technology—Personal information security specification], www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf (accessed on September 10, 2019).

24. On February 16, 2016, the US District Court for the Central District of California ordered Apple Inc. to provide required software to allow the Federal Bureau of Investigation to break into an Apple iPhone 5C belonging to a shooter involved in the December 2015 San Bernardino attack. In an open letter published the same day, Apple CEO Tim Cook refused to build a backdoor to the iPhone that could allow the US government to unlock and access any iPhone. On March 28, 2016, the US government vacated the order, claiming that the government unlocked the iPhone with assistance from an unnamed third party. The court order is available at www.justice.gov/usao-cdca/file/825001/download, Tim Cook's message to customers is available at www.apple.com/customer-letter/, and the government statement to drop the court order is available at www.justice.gov/usao-cdca/pr/statement-united-states-attorney-eileen-m-decker-government-request-vacate-order (all accessed on June 29, 2019).

25. According to the *Washington Trade Daily*, China and Russia raised concerns about the prohibition that the United States and the European Union advocate ("Debate on Source Code," August 5, 2019). Another related issue is China's restrictions on wholly foreign-owned IT service providers handling or storing data on local users. Some companies claim they cannot directly provide cloud storage services but must turn those activities over entirely to their domestic joint venture partners in China.

26. See Claude Barfield, "TPP a model for NAFTA digital trade rules," East Asia Forum, December 8, 2017, www.eastasiaforum.org/2017/12/08/tpp-a-model-for-nafta-digital-trade-rules/ (accessed on July 3, 2019).

It should be possible to bridge the US and EU positions on source code. China is a question mark.

Customs Duties

At the 1998 WTO Ministerial Conference, members adopted the Declaration on Global Electronic Commerce, committing to continue the practice of zero customs duties on electronic transmissions. Subsequent ministerial conferences renewed the commitment, with the latest declaration adopted in Buenos Aires in December 2017. All the three giant economies currently oppose customs duties on digital products. However, the Chinese proposal advocates zero tariffs only until the next WTO ministerial conference, to be held in June 2020 in Kazakhstan. A possible interpretation is that, unless the WTO declaration is renewed, China could impose customs duties on digital products.

Meanwhile, India and South Africa have questioned the zero-customs-duty rule and view customs duties on digital products as a potential revenue source. They argue that rapid development of digital trade will lower the share of traditional trade and erode customary tariff revenues.[27] Accordingly, members should conduct a deeper assessment of the revenue aspect of the zero-customs-duty rule and analyze its influence on the ability of developing and least developed countries to adopt digital technology.[28]

Internet Taxes

This topic is not explicitly addressed in EU and US proposals, but discussions and disputes have already started.[29] The gap between US and EU positions on internet taxation is big, and reconciliation is not promising. China's position on it is unknown.

For years, the European Union has complained that large US multinational corporations (MNCs) operating in Europe do not pay a fair share of corporate taxes to EU member states. An unrelated EU complaint about US MNCs is that tech firms are too often monopolistic.[30] State aid cases, hinging on tax issues surrounding the transfer pricing arrangements of US firms, include Apple's dispute with the European Union regarding its tax agreements with Ireland and the tax deals of Amazon and McDonald's with Luxembourg.[31]

In this spirit, the Organization for Economic Cooperation and Development (OECD) initiated the Base Erosion and Profit Shifting (BEPS) project after the 2012 G-20 Summit in Mexico. The project aims to combat tax avoidance and improve the coherence of international tax rules. Building on the BEPS project, the European Commission in 2018 proposed both a digital services tax and a digital profits tax that would respectively target slices of large technology firms' revenue and profits that are arguably attributable to EU member states (Hufbauer and Lu 2018). The rationale is that local users contribute value to digital platforms. Therefore, the jurisdiction where users reside (i.e., EU member states) should have the right to tax firms on a slice of their revenues or profits, no matter where the firm is located (usually the United States). However, high thresholds of revenue or profit that the European Union proposes before a firm is subject to the new taxes would clearly discriminate against US tech giants such as Google and Facebook.

The gap between US and EU positions on internet taxation is big, and reconciliation is not promising. China's position on it is unknown.

Although new global tax rules are urgently needed to deal with challenges in the digital era, rules should be designed through multilateral consultation rather than unilateral legislation. While the OECD ambitiously hopes to conclude a

27. Makiyama and Narayanan (2019) from the European Center for International Political Economy argue that countries would lose more in GDP than they would gain in tariff revenues if the WTO e-commerce moratorium is lifted.

28. See "India, South Africa: WTO e-commerce moratorium too costly for developing members," *Inside U.S. Trade*, June 5, 2019, https://insidetrade.com/daily-news/india-south-africa-wto-e-commerce-moratorium-too-costly-developing-members (accessed on June 29, 2019).

29. Article 19.4 on "Non-Discriminatory Treatment of Digital Products" in the USMCA implicitly touches the issue of internet taxes.

30. Apart from tax avoidance, the European Union has been blaming US MNCs for their abuse of dominant market positions. On March 20, 2019 the European Commission fined Google €1.49 billion for breaching EU antitrust rules, after fining the company €2.42 billion in 2017 and €4.34 billion in 2018 for anticompetitive behaviors. See "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising," European Commission, March 20, 2019, http://europa.eu/rapid/press-release_IP-19-1770_en.htm (accessed on June 29, 2019). In addition, the Commission may open an antitrust investigation against Amazon; see "A full EU probe into Amazon could come in the next few months, top official says," CNBC, April 3, 2019, www.cnbc.com/2019/04/03/eus-vestager-says-a-full-probe-into-amazon-could-come-before-october.html (accessed on June 29, 2019). Moreover, Spotify filed an antitrust complaint against Apple with EU antitrust regulators; see "Spotify files EU antitrust complaint against Apple," Reuters, March 13, 2019, www.reuters.com/article/us-apple-spotify-tech-eu/spotify-files-eu-antitrust-complaint-against-apple-idUSKBN1QU18G (accessed on June 29, 2019).

31. See Hufbauer and Lu (2016) for the Apple case.

multilateral agreement by 2020, the uncoordinated proliferation of digital services taxes could complicate the landscape and jeopardize tax cooperation (IMF 2019).

The United States forcefully objects to the unilateral EU digital tax proposals, citing potential violations of tax treaties and other agreements. Most recently, after the French National Assembly and Senate passed the country's 3 percent digital services tax, the Office of the United States Trade Representative initiated a Section 301 investigation against the tax on July 10, 2019.[32] The two countries reached a provisional deal at the G-7 Summit in August, after France promised to reimburse companies for digital taxes paid once OECD members agree on prospective new rules governing international taxation.[33] Industry sources claim that the United States agreed to suspend its Section 301 investigation only for 90 days. Most recently in September 2019, the United States reached a high-standard and comprehensive deal with Japan on digital trade.[34] Apart from subjects of free data flows, prohibition of data localization, allowing technology companies to use encryption to protect privacy, prohibition of forced technology transfer, and no customs duties, the agreement explicitly specified that nondiscriminatory treatment of digital products includes the coverage of tax measures. The United States fears that additional countries may follow the French initiative and levy their own digital revenue taxes if there is no deadline on US forbearance.[35]

32. In March 2019, France introduced a digital services tax of 3 percent to be applied on companies that have worldwide revenue of at least €750 million per year and taxable revenue from taxable services in France of at least €25 million per year. The bill was passed into law on July 24, 2019, and applies retroactively to January 1, 2019. For legislative history, see "Création d'une taxe sur les services numériques [Creation of a tax on digital services]," Sénat, www.senat.fr/dossier-legislatif/pjl18-452.html (accessed on June 30, 2019). For the US Section 301 investigation against France, see "USTR Announces Initiation of Section 301 Investigation into France's Digital Services Tax," USTR, July 10, 2019, available at https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/july/ustr-announces-initiation-section-301.

33. See "Macron says France and U.S. reached digital tax deal," Reuters, August 26, 2019, www.reuters.com/article/us-g7-summit-tax-macron/macron-says-france-and-u-s-reached-digital-tax-deal-idUSKCN1VG1N7 (accessed on August 29, 2019).

34. See "Fact Sheet: U.S.-Japan Trade Agreement," Office of the United States Trade Representative, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/september/fact-sheet-us-japan-trade-agreement (accessed on September 30, 2019).

35. Justifying US apprehension, on October 1, 2019, in the midst of a parliamentary campaign, Canadian Prime Minister Justin Trudeau floated a French-style digital tax for Canada. Such a tax would probably be inconsistent with the USMCA, but that pact is not yet ratified, and in any event the prohibition on digital taxes in the USMCA is not as tight as the prohibition in the US-Japan trade deal. See "Trudeau floats French-style digital services tax for Canada," *Inside U.S. Trade*, October 1, 2019, https://insidetrade.com/daily-news/trudeau-floats-french-style-digital-services-tax-canada?s=iust (accessed on October 6, 2019).

36. See "Value Added by Industry: Value Added by Industry as a Percentage of Gross Domestic Product (A) (Q)," Bureau

OECD members could engage in very long deliberations before reaching a multilateral agreement.

Open Internet Access

Not surprisingly, the European Union and the United States advocate generally open internet access for residents of WTO member states. However, under public pressure in the United States and legal pressure in some EU member states, website hosts—notably but not only Google—block websites that purvey hate, pornographic, or terrorist content. In sharp contrast to Western values, China exerts strong state control over cyberspace, illustrated by the Great Firewall. The Firewall regulates the internet by filtering content and blocking websites that feature "sensitive" topics, including for example the *Wall Street Journal* and *New York Times*. Citing internal security, China emphasizes internet sovereignty along with other cyberspace controls. This will be a hard gap to bridge.

Other Issues

The United States, the European Union, and other advanced economies aim to conclude an ambitious high-standard WTO e-commerce agreement, while China emphasizes the development dimension of e-commerce. Beijing argues that developing countries—a characterization with which China has self-identified in the WTO—should receive special and differential treatment. The United States strongly opposes China's self-declared developing-country status, and this opposition would extend to negotiations on new e-commerce rules when China attempts to exempt itself from certain commitments by citing its developing-country status. As a general matter, and a persistent stumbling block in Doha Round negotiations, the United States argues that "special and differential treatment" for self-identified developing countries has been seriously abused in the WTO system.

Regarding the definition of "digital products," the United States insists on including audiovisual wares, while the European Union wants to exclude them from the negotiation. The financial well-being of film and music creators—an industry that accounted for 0.5 percent of US GDP in 2018—rests on this issue.[36] Hollywood might well oppose any e-commerce agreement that excludes its wares.

The Chinese position on this issue is probably aligned with that of the European Union.[37]

As for "net neutrality"—the proposition that all internet users should share equal priority to proprietary transmission systems—there is wide disagreement between the United States and the European Union. Under the Trump administration, the Federal Communications Commission discarded net neutrality, meaning that internet platforms can now sell priority access to their transmission systems. In Europe, net neutrality is guaranteed by EU Regulation 2015/2120. Almost certainly the e-commerce negotiations will leave this matter to individual countries.

Finally, Article 19.17 of the United States-Mexico-Canada Agreement (USMCA) stipulates that parties cannot impose liability on the supplier of interactive computer services (e.g., a platform such as Facebook) unless the supplier engaged in creating information that inflicted harm.[38] This differs from the internet service provider (ISP) safe harbor in the erstwhile Trans-Pacific Partnership (TPP) Articles 18.81 to 18.82, which limited ISP liability for inadvertent infringement of intellectual property rights.[39] That ISP section was suspended in the CPTPP, signed by Mexico and Canada, among others. In any event, the TPP limit on ISP liability differs from the interactive computer services provision in the USMCA. The United States will probably advocate some version of limited ISP liability in e-commerce talks. The positions of the European Union and China on this issue are unknown.

OUTLOOK FOR E-COMMERCE TALKS

The prospect of reaching a high-level WTO e-commerce agreement is not promising. While the recent US-Japan trade deal ensures that the United States and Japan are on the same page, big differences separate the other major powers. The United States and the European Union have major differences on internet taxes, privacy, and whether to include audiovisual products in the negotiation. China seems unwilling to commit on data flows, data localization, and transfers of source code. Although China sides with the European Union on privacy concerns, on other contentious issues—including open internet access and the depth of a WTO e-commerce agreement—it holds opposite views from the European Union and the United States.

Meanwhile, national views are evolving. The United States, for example, is becoming more security conscious while, at the same time, some consumer advocates are placing a higher value on individual privacy.[40] Shifting views will complicate international negotiations.

Accordingly, the outlook is dim for e-commerce talks to deliver a robust plurilateral agreement among the 76 launch countries. G-20 countries have declared that they will seek to encourage "interoperability of different frameworks," a commitment that promises nothing while masking substantive discord.[41]

If an agreement is to be reached, either its scope must be sharply narrowed to exclude most of the contentious issues or the number of participating countries must be sharply reduced. A WTO accord, even of low ambition, would have value if only to establish basic digital norms on matters such as banning unsolicited commercial messages, ensuring the validity of electronic contracts, and protecting online consumers from fraudulent practices. A more ambitious accord, covering controversial questions such as server location (i.e., data localization), free access to the internet, and the sanctity of source code, should be the subject of bilateral and/or plurilateral/regional pacts, rather than multilateral WTO negotiations.

---

of Economic Analysis, https://apps.bea.gov/iTable/iTable.cfm?ReqID=51&step=1 (accessed on August 29, 2019).

37. China and the United States litigated a WTO case on audiovisual products back in 2007; see "DS363: China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products," World Trade Organization, www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm (accessed on June 30, 2019). Although the case is about market access rather than the definition of "digital products," it suggests that China would not be sympathetic to include audiovisual wares in e-commerce negotiations.

38. The USMCA grants Mexico a phase-in period of 3 years for this article.

39. ISP liability was addressed in Chapter 18: Intellectual Property of the TPP.

40. See, for example, "Consumer, Privacy, Civil Rights Groups Tell Congress That States Must Have Power to Safeguard Privacy," Public Citizen, December 13, 2018, www.citizen.org/news/consumer-privacy-civil-rights-groups-tell-congress-that-states-must-have-power-to-safeguard-privacy/ (accessed on September 16, 2019).

41. See "G-20 Ministerial Statement on Trade and Digital Economy," https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf (accessed on June 30, 2019). The G-20 Osaka Leaders' Declaration also mentions the same idea. See "G-20 Osaka Leaders' Declaration," www.g20.org/pdf/documents/FINAL_G20_Osaka_Leaders_Declaration.pdf (accessed on July 3, 2019).

REFERENCES

Biancotti, Claudia, and Paolo Ciocca. 2019. *Opening Internet Monopolies to Competition with Data Sharing Mandates*. PIIE Policy Brief 19-3. Washington: Peterson Institute for International Economics.

Casalini, Francesca, and Javier López González. 2019. *Trade and Cross-Border Data Flows.* OECD Trade Policy Papers No. 220. Paris: Organization for Economic Cooperation and Development.

Cory, Nigel. 2017. *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Washington: Information Technology & Innovation Foundation.

Hofheinz, Paul, and Michael Mandel. 2015. *Uncovering the Hidden Value of Digital Trade.* Interactive Policy Brief Issue 19/2015. Brussels: The Lisbon Council.

Hufbauer, Gary, and Euijin Jung. 2016. *The US-EU Privacy Shield Pact: A Work in Progress.* PIIE Policy Brief 16-12. Washington: Peterson Institute for International Economics.

Hufbauer, Gary Clyde, and Zhiyao (Lucy) Lu. 2016. *Apple's Tax Dispute with Europe and the Need for Reform.* PIIE Policy Brief 16-16. Washington: Peterson Institute for International Economics.

Hufbauer, Gary Clyde, and Zhiyao (Lucy) Lu. 2018. *The European Union's Proposed Digital Services Tax: A De Facto Tariff.* PIIE Policy Brief 18-15. Washington: Peterson Institute for International Economics.

IMF (International Monetary Fund). 2019. *Corporate Taxation in the Global Economy.* Washington.

Makiyama, Hosuk-Lee, and Badri Narayanan. 2019. *The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions.* Policy Brief No. 3/2019. Brussels: European Center for International Political Economy.

McKinsey Global Institute. 2016. *Digital Globalization: The New Era of Global Flows.* New York: McKinsey & Company.

USITC (United States International Trade Commission). 2014. *Digital Trade in the U.S. and Global Economies, Part 2.* Publication Number 4485. Washington.

Zhang, Longmei, and Sally Chen. 2016. *China's Digital Economy: Opportunities and Risks.* IMF Working Paper WP/19/16. Washington: International Monetary Fund.