CHAPTER

6 DIGITAL SERVICES TRADE AND TRADE AGREEMENTS

Henry Gao

Trade agreements have become the main forum for the regulation of digital services trade issues over the past decade. This chapter provides a comprehensive examination of the regulation of digital services trade in trade agreements, first reviewing the rules in the World Trade Organization (WTO), then comparing the approaches between the United States (US), the People's Republic of China (PRC), and the European Union (EU), and explaining the reasons for their deep differences. This chapter further analyzes such provisions in trade agreements in Asia and the Pacific, which has become one of the most dynamic regions in terms of new regulations on digital trade issues, with a mix of digital services trade chapters in regional and bilateral free trade agreements. By drawing lessons from existing agreements, the chapter also illustrates how economies in the region may further develop digital services trade.

6.1 Regulation of Digital Services in the World Trade Organization[1]

Pending eventual negotiations of new disciplines in the WTO, the main obligations for the regulation of digital trade or e-commerce[2] under the WTO legal framework can be found in the General Agreement on Trade in Services (GATS) and in the GATS Reference Paper on Telecommunications (reference paper). The reference paper sets out the basic rights for access to and the use of public telecommunications networks and services by services suppliers, including e-commerce suppliers (WTO 1994). The general principle is that services

[1] This section is largely based on Gao (2017).

[2] E-commerce and digital trade are often used interchangeably. But, as noted at the outset of this chapter, the Organisation for Economic Co-operation and Development's definition of e-commerce (which covers only digitally ordered trade) differs from the WTO definition, which also covers digital delivery of services. Therefore, the term e-commerce is sometimes used in this chapter to refer only to e-commerce for goods. The chapter otherwise refers to e-commerce for services (e-services) or more often to digital services trade including data flows.

suppliers shall be able to access and use public telecommunications networks and services on reasonable and nondiscriminatory terms and conditions. This principle is elaborated to strike a delicate balance between users' rights (para. 5 lit. b and c) and regulators' rights (para. 5 lit. e-g).[3] Another key discipline to consider on regulating trade in digital services is the WTO Moratorium on Customs Duties on Electronic Transmissions (Box 6.1).

Box 6.1: The Evolution of Digital Services in the World Trade Organization

World Trade Organization (WTO) members adopted a Declaration on Global Electronic Commerce at the 2nd WTO Ministerial Conference (MC) in May 1998. The declaration focused on the establishment of a comprehensive work program on "all trade-related issues relating to global electronic commerce," and a WTO moratorium on customs duties on electronic transmissions (WTO 1998).

World Trade Organization Work Programme on Electronic Commerce

Under the WTO Work Programme on Electronic Commerce, adopted by the General Council in September 1998, "electronic commerce" covers "the production, distribution, marketing, sale or delivery of goods and services by electronic means" (WTO 1998). Its scope also includes "issues relating to the development of the infrastructure for electronic commerce." Responsibilities are divided among different WTO bodies required to report progress to the General Council on a regular basis.

- **The Council for Trade in Services** is responsible for examining the treatment of e-commerce in the General Agreement of Trade in Services (GATS) legal framework, including horizontal issues such as the scope and classification of sectors, access to and use of public telecommunications transport networks and services, and the application of core unconditional obligations (most favored nation, transparency) and discretionary negotiated commitments (market access, national treatment, domestic regulations).
- The **Council for Trade in Goods** is tasked with examining aspects of e-commerce relevant to the provisions of the General Agreement on Tariffs and Trade (GATT) 1994, the agreements covered under Annex 1A of the WTO Agreement, and the approved work program, which include tariff-related issues, and nontariff issues such as rules of origin, customs valuation, and import licensing and standards.
- The **Council for Trade-Related Aspects of Intellectual Property Rights** deals with intellectual property issues arising in connection with e-commerce (protection and enforcement of copyright and trademarks, access to technology).
- The **Committee on Trade and Development** reviews and reports on the development implications of e-commerce, taking into account the economic, financial, and development needs of developing countries.

continued on next page

[3] Gao (2008) presents a detailed discussion on this principle.

Box 6.1 *continued*

- The **General Council** is responsible for the review of any crosscutting trade-related issues and all aspects of the work program concerning the imposition of customs duties on electronic transmissions.

Moratorium on Customs Duties

The "practice of not imposing customs duties on electronic transmissions" has been extended repeatedly since 1998, with the latest extension in June 2022 at MC 12 that will remain in effect until the next WTO ministerial conference or until 31 March 2024 should MC 13 be postponed beyond that date.[a] This moratorium nevertheless left a few questions unanswered.

- Does the term "electronic transmissions" refer only to the medium of e-commerce, or to the content of the transmission as well, i.e., the underlying product or service being transmitted?
- If it refers to the medium of transmission only, could other digital products supplied via traditional mediums, such as books, music, or videos on CDs, be subject to customs duties?
- Does the prohibition apply only to customs duties, or does it extend to other fees or charges imposed on the digital products?
- Does the moratorium apply only to imports or also to exports?

Although contested, the moratorium is widely cited by the global services business community as having been fundamental in support of innovation and growth in digital services, and some WTO members have made commitments in regional trade agreements to ban customs duties on e-transmissions.

Notwithstanding the ambitious agenda in the work program, WTO members were unable to reach any decisions on new substantive disciplines on e-commerce (WTO 2013). This changed at the 11th Ministerial Conference in December 2017, when 71 members led by three co-conveners—Australia, Japan, and Singapore—made a joint statement to "initiate exploratory work together toward future WTO negotiations" on e-commerce. The plurilateral negotiations started formally in January 2019 and at the time of writing, 86 members are participating.

[a] WTO. MC12 Briefing Note: E-commerce. https://www.wto.org/english/thewto_e/minist_e/mc12_e/briefing_notes_e/bfecom_e.htm#:YwyWcHYykv8 (accessed 30 August 2022).

Source: Gao (2017).

Beyond the rules in the telecoms reference paper, the issues involved in the regulation of digital trade in the WTO fall largely into three areas: classifications, obligations, and exemptions.

This chapter presents a preview of three main approaches, each embodied by the regulatory experiences of the US, the EU, and the PRC, and each focusing on different aspects of digital services trade. With these models in mind, attention

then shifts specifically to Asia and the Pacific, with a comprehensive mapping of 53 free trade agreements (FTAs) in the region that include chapters on digital trade issues. Lessons are drawn over gaps identified in these agreements, as well as on how economies in Asia and the Pacific may improve their digital trade chapters to better harness opportunities for digital services trade.

6.1.1 Classifications

Internet activities can be classified as goods or services (Wunsch-Vincent and Hold 2012). The distinction is not merely theoretical; it has profound practical implications. If internet activities are treated as goods, they could be subject first and foremost to customs duties, as well as most favored nation (MFN), national treatment, and an entire set of nontariff disciplines such as those on rules of origin, import licensing, customs valuation, and so on. On the other hand, if they are treated as services, the members would be unable to regulate them through border measures such as tariffs, but would have significant leeway in imposing domestic regulations. While some activities such as the online delivery of books and audiovisual products could arguably be classified as goods, according to the technology-neutrality principle,[4] most activities carried through the internet share more similarities with services trade. For example, many e-commerce activities such as online shopping and gaming are intangible and non-storable like services. Similarly, many e-commerce activities such as online search and e-mail involve joint inputs from suppliers and consumers, and so are tailored to the needs of specific consumers like other services.

Focusing on services, the GATS takes a different regulatory stance to the General Agreement on Tariffs and Trade (GATT), which applies a uniform set of rules to most products. According to the GATS "positive listing" approach, WTO members only assume obligations with respect to sectors they have included in their schedule of specific commitments.[5] Therefore, to determine whether a given e-commerce activity is covered, one has to determine which sector or subsector such activity falls under and then examine the respective schedules.

Services are classified under the GATS according to the Services Sectoral Classification List, which puts all services into 12 sectors and 160 subsectors (WTO 1991). While this system does a good job in classifying most other services sectors, it has not been so useful in classifying e-commerce activities. To start with, the classification list is outdated as it is based on the United Nations Provisional

[4] As noted by the WTO Secretariat, "the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied" (WTO 1999).

[5] WTO. General Agreement on Trade in Services. Article XVI: Market Access. https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm.

Central Product Classification (CPCprov).[6] The CPCprov was published in 1990, when the internet was still in its infancy and many e-commerce activities, such as search engines, did not even exist. It does not provide direct reference to many e-commerce activities common today. Instead, they are often scattered across sectors. For example, search engine services can arguably be classified under either telecommunication services or computer and related services. Paradoxically, some classifications under the Services Sectoral Classification List also overlap with each other. For example, under the list, online info processing and data processing share the same code under CPCprov, but info processing is grouped under telecommunication services and data processing under computer services.

To better capture the reality of e-commerce activities, the classification system needs to be reviewed and revamped.[7] Different approaches should be taken, depending on the nature of the services. On the one hand, e-commerce activities supplied through traditional channels before the advent of the internet should be grouped under the original sector as per the technology-neutrality principle, unless online delivery has changed their nature.[8] Thus, online banking services should be classified under banking services, and online universities should be classified under educational services, and so on. On the other hand, the classification of services that only emerged with the birth of the internet is trickier. Given that the latest version of the Central Product Classification (CPC) includes many such services, it is tempting to simply replace the reference to the CPCprov codes in the Services Sectoral Classification List with the corresponding codes in the new version. However, this approach is undesirable. First, as the Services Sectoral Classification List is not mandatory, not every WTO member uses it or includes explicit reference to the CPC codes in its schedule.[9] Second, even where the CPC is used, the schedule cannot be simply updated with the new CPC versions. This is because the CPC often reshuffles the code numbers around when the versions are updated, thus the same code numbers under different versions

[6] United Nations. 1991. Provisional Central Product Classification. *Statistical Papers.* Series M. No. 77. New York. http://unstats.un.org/unsd/CR/Registry/regcst.asp?Cl=9&Lg=1.

[7] Tuthill and Roy (2012) provide an overview of the classification issues for e-commerce.

[8] Peng (2016) discusses the application of the technology-neutrality principle to e-commerce activities.

[9] Notably, the US does not use the CPC code in its classification, see WTO (1994). However, while the US schedule makes no explicit references to CPC numbers, it corresponds closely with the GATT Secretariat's list (USITC 1998). This issue was also debated in the US-Gambling case (WTO 2005).

might refer to entirely different services.[10] Third, as cases like US-Gambling have shown, WTO members have found it challenging to understand even their own commitments (WTO 2005). Thus, they will not accept a comprehensive update of the schedules without careful scrutiny.

Because of these difficulties, even an update of the schedules based on the latest CPC version probably cannot be achieved without major negotiation efforts. In addition, as many e-commerce activities are closely linked, it is probably better to take a cluster approach in the review and deal with them together.[11]

6.1.2 Obligations

A WTO member may choose among different levels of liberalization even for services covered in its schedule. It may do so by inscribing commitments ranging from "none" (which means "no limitation" or "fully liberalized") to "unbound" (which means "no commitment") in the market access and national treatment columns (WTO 2001). Thus, determining a member's specific obligations with respect to e-commerce activities requires examining the specific wording of that member's schedule.

Other than general rules such as the MFN principle, most substantive obligations under the GATS only apply when a member schedules relevant commitments. The member may choose the level of market access[12] and/or national treatment[13] it is willing to offer for each sector included in its schedule. Moreover, such scheduled commitments are also subject to sector- or mode-specific limitations. This regulatory framework creates several problems for e-commerce activities.

First is ambiguity in sectoral coverage. Even though a member may choose which sectors to include in its schedule, ambiguities could still arise due to imperfections in the classification system. A good example is the US-Gambling dispute. In this dispute, the US included in its schedule a subsector entitled

[10] A good example is the classification of data processing services (CPC 843) under CPCprov and CPC Ver.1, which is discussed in Gao (2012).

[11] The cluster approach was proposed by the US and the EU in 2000 (WTO 2000a, 2000b). This approach grew out of an initial proposal by the Dominican Republic, El Salvador, and Honduras for an annex on tourism in the GATS described in Raghavan (2000).

[12] GATS Article XVI.1 states, "With respect to market access through the modes of supply identified in Article I, each Member shall accord services and service suppliers of any other Member treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule."

[13] GATS Article XVII.1 states, "In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers."

"Other Recreational Services (except sporting)." While the US argued that "sporting" includes gambling services, the WTO Panel disagreed and ruled that sporting does not include gambling services and so should be included in the US commitments (WTO 2005). While this problem could arise in any services sector, e-commerce activities are particularly prone to interpretive ambiguities because of the classification difficulties mentioned earlier.

The second problem is confusion on modes of supply. Under the GATS, services could be supplied in four modes: (i) cross-border supply, (ii) consumption abroad, (iii) commercial presence, and (iv) movement of natural persons.[14] For e-commerce activities, it is quite difficult to tell if a service is supplied through mode 1 or 2 given that the service is provided in cyberspace (WTO 1998; Wunsch-Vincent and Hold 2012). Further complications could arise when the service supplier is located in another WTO member but maintains a server in the home economy of the consumer. In such cases, it could be argued that mode 3 should apply. As a member may have different levels of commitments depending on the mode of supply, confusion over the mode of supply could create illogical consequences.

To address these problems, it would benefit WTO members to agree on a set of scheduling guidelines for e-commerce activities. This would help clarify the meaning of schedules and avoid future complications. A set of principles on a minimum regulatory standard for e-commerce activities should also be formulated. The GATS Reference Paper on Telecommunications (WTO 1996) provides a good model given the close links between the two sectors.[15]

6.1.3 Exceptions

Legitimate policy reasons may lead WTO members to deviate from their trade obligations. Such deviations are permitted by both the GATT and the GATS through "General Exceptions" clauses.[16] However, as illustrated by the record of WTO disputes, the preferred exceptions under each agreement are rather different. The most commonly cited exceptions under the GATT, are the ones to

[14] GATS Article 1.2 states, "For the purposes of this Agreement, trade in services is defined as the supply of a service: (a) from the territory of one Member into the territory of any other Member; (b) in the territory of one Member to the service consumer of any other Member; (c) by a service supplier of one Member, through commercial presence in the territory of any other Member; and (d) by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member."

[15] Kariyawasam (2012) gives an example on how the reference paper can be revised to apply to internet networks.

[16] GATT 1994 Article XX and GATS Article XIV.

protect public health and the environment.[17] Under the GATS, the most frequently invoked clause has been the public morals exception in Article XIV(a).[18]

Interestingly, in two cases concerning internet services, i.e., *US–Gambling* and *China–Publications and Audiovisual Products,* respondents cited the public morals exception to defend their measures. In their rulings, the panels and the Appellate Body give national authorities wide discretion in defining both the boundaries and depth of the exception, but this could lead to bizarre results (WTO 2005, 2010). For example, in *China–Publications and Audiovisual Products,* the Appellate Body encouraged the PRC government to conduct censorship itself as, from the perspective of WTO law, this could supposedly be less trade-restrictive than outsourcing censorship to private firms.[19]

A good way to prevent the potential abuse of the exception is to adopt some universal benchmark on what may qualify as public morals, so that fundamental human rights, such as those enshrined in the Universal Declaration of Human Rights,[20] will not be harmed under the guise of protection of public morals. As the core competence of the WTO is in trade, it is ill-equipped for this task. Instead, members should consider adopting a mechanism similar to the one that exists under the Sanitary and Phytosanitary (SPS) Agreement—that is, having the standards formulated by another international organization[21] with competence

[17] GATT 1994 Article XX(b) and (g). Article XX(b) was invoked in disputes such as the *European Communities—Measures Affecting Asbestos and Asbestos-Containing Products* (DS135); *Brazil—Measures Affecting Imports of Retreaded Tyres* (DS332); *European Communities—Measures Prohibiting the Importation and Marketing of Seal Products* (DS400, DS401); *United States—Measures Affecting the Production and Sale of Clove Cigarettes* (DS406); and *Indonesia—Importation of Horticultural Products, Animals and Animal Products* (DS477, DS478). Article XX(g) was invoked in disputes such as *United States—Standards for Reformulated and Conventional Gasoline* (DS2); *China—Measures Related to the Exportation of Various Raw Materials* (DS394, DS395, DS398); and *Measures Related to the Exportation of Rare Earths, Tungsten and Molybdenum* (DS431, DS432, DS433).

[18] GATS Article XIV(a) has been invoked in disputes such as *US–Gambling* (WTO 2005) and *China–Publications and Audiovisual Products* (WTO 2010).

[19] In this case, the US proposed that, instead of having the importing firms conduct the content review of imported publications, the PRC government shall be given sole responsibility for conducting content review. Both the Panel and the Appellate Body agreed that these are reasonably available alternatives (WTO 2010). Delimatsis (2012) includes a discussion on the Panel and Appellate Body decisions on *China—Publications and Audiovisual Products.*

[20] United Nations. Universal Declaration of Human Rights (1948). https://www.ohchr.org/en/resources/educators/human-rights-education-training/universal-declaration-human-rights-1948.

[21] The WTO Agreement on the Application of Sanitary and Phytosanitary Measures (SPS Agreement), Annex A, para. 3, refers explicitly to the SPS standards, guidelines, and recommendations made by various international organizations such as the Codex Alimentarius Commission, the International Office of Epizootics, and the Secretariat of the International Plant Protection Convention.

on public morals issue, and making it mandatory for the WTO to consult them when disputes arise.[22]

Due to its unique nature, e-commerce activities pose special challenges to the GATS regulatory framework on all three issues. While the GATS, in its current form, is not well suited to the regulation of e-commerce, it can keep up with the regulatory task. However, to make this happen, new approaches are needed for dealing with e-commerce activities, especially on key issues such as classifications, obligations, and exceptions.

In this regard, the WTO can learn from the approaches taken in the various FTAs, which are discussed in the next section.

6.2 Regulation of Digital Services Trade: Three Models[23]

Any framework for digital trade regulation would involve three groups of players: the individual, who provides the raw data and uses the processed data; the firm, which processes raw inputs from the consumer, and usually controls such data; and the state, which monitors and regulates the data used by the first two groups. Their different interests often result in conflicting priorities, with the individual advocating privacy protection, the firm promoting unhindered data flow, and the state focusing on the security implications.

While all regulators would agree on the need to strike a balance between the clashing interests of different stakeholders, their approaches often differ in practice. Some jurisdictions prioritize the need to safeguard the privacy of users. A good example in this regard is the General Data Protection Regulation (GDPR) of the EU, which recognizes "[t]he protection of natural persons in relation to the processing of personal data" as "a fundamental right."[24] On the other hand, some jurisdictions put the commercial interests of firms first. In the US, this is reflected in the 1996 Telecommunication Act, which notes that it is "the policy of the United

[22] SPS Agreement Article 11.2 gives the right to dispute settlement panels to consult the relevant international organizations on scientific or technical issues; whereas, SPS Agreement Article 12.3 requires the SPS Committee to "maintain close contact with the relevant international organizations in the field of sanitary and phytosanitary protection … with the objective of securing the best available scientific and technical advice for the administration of this Agreement."

[23] This section is largely based on Gao (2021).

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018, Recital 1.

States ... to preserve ... free market ... unfettered by Federal or State regulation."[25] In contrast, national security concerns are often cited to justify restrictions on cross-border data flows, though to varying degrees in different economies. A recent example is the PRC's 2017 Cybersecurity Law, which imposed several restrictions aiming to "safeguard cybersecurity, protect cyberspace sovereignty, and national security."[26] These divergent approaches are also reflected in the trade agreements concluded by the three main players.

6.2.1 United States

As the world's largest economy and, until recently, the largest trader, the US is a highly competitive exporter in both agricultural and industrial goods and services. It has been promoting free trade and dismantling barriers in its trade agreements. This approach is also carried over into the digital age, with US trade agreements pioneering the inclusion of digital trade issues with an expansive set of obligations.

In particular, two provisions have become essential parts of the digital trade chapters in US trade agreements, with the recently concluded US–Mexico–Canada Agreement (USMCA) as the most prominent example: the first provision is the guarantee on free cross-border flow of data by stating that "no Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means" (Article 19.11); and the second is the prohibition of data localization requirements by stipulating that "no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory" (Article 19.12).[27]

Both provisions provide strong protection of the interests of the firm, deeming restrictions on cross-border flow of data and various localization requirements as obstacles to conducting business across national boundaries.

As will be seen from the experiences of the PRC and the EU, two of the most frequent reasons used by governments to regulate data are protection of privacy or national security. In both of these areas, however, the US has taken somewhat different approaches in its trade agreements.

On privacy protection, US trade agreements only require parties to adopt their own legal framework for data protection, which could take many different legal

[25] Telecommunication Act of 1996, 47 U.S.C. 230(b)(2). https://www.law.cornell.edu/uscode/text/47/230 (accessed 20 February 2020).

[26] Cybersecurity Law of the People's Republic of China [*Zhonghua Renmin Gongheguo Wangluo Anquan Fa*], as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on 7 November 2016, Art. 1.

[27] Office of the United States Trade Representative. Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text. https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

approaches, including "comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy" (USMCA footnote 4). This is very different from the EU approach, where trade partners are required to adopt GDPR-equivalent clauses. While the US agreements also call for parties to "take into account principles and guidelines of relevant international bodies" (USMCA Article 19.8.2), the examples only include the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the Organisation for Economic Co-operation and Development Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), which are regarded as providing minimum levels of data protection or "first generation" data privacy standards (Greenleaf 2018).

The US trade agreements seem to be relatively more concerned with making sure that the commercial interests of firms are not hurt by over-restrictive privacy regimes. Take for example the clause on personal information protection under the USMCA, which covers six paragraphs. One of these contains substantive obligations to adopt or maintain legal framework on personal information protection (Article 19.8.2), while three are aimed at minimizing the regulatory burden for businesses. The first among the three calls the parties to ensure that "any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented" (Article 19.8.3), which are apparently modeled after the necessity test and proportionality principle under the WTO. The second requires parties to "endeavor to adopt nondiscriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction," which also draws from the nondiscrimination principle of the WTO, especially the national treatment obligation. Last, while the agreement recognizes the varying legal approaches parties might take on personal information protection, it also encourages them to develop "mechanisms to promote compatibility between these different regimes." Again, trade lawyers would recognize in these provisions vestiges of rules on mutual recognition, harmonization, and equivalence under various WTO agreements.

On security, the US trade agreements focus on "threats to cybersecurity [that] undermine confidence in digital trade"—i.e., "malicious intrusions or dissemination of malicious code that affect electronic networks" (USMCA Article 19.15). Put differently, the US approach mainly focuses on cybersecurity risks facing the private sector, which is quite different from the PRC approach that focuses on perceived threats to national security. At the same time, the US approach also tries to minimize disruptions to the operations of firms, by calling parties to adopt "risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks" (USMCA Article

19.15). The risk-based approach is carried over from the regulatory framework under the WTO, especially under the agreements on technical barriers to trade and sanitary and phytosanitary measures. By placing restrictions on the regulatory measures that governments might adopt, such an approach provides better protection for firms' businesses. Similarly, the reference to "consensus-based standards" also reflects practices in the US that were codified in the Cybersecurity Enhancement Act of 2014.[28] The act calls for the National Institute for Standards and Technology under the Commerce Department to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost effectively reduce cyber risks to critical infrastructure."[29] Under the act, US cybersecurity standards are developed as a partnership between the government and the private sector, which serves to reduce the cybersecurity risks for the firms.

Many other provisions in the USMCA are also designed to help develop digital trade. This is done by either removing regulatory barriers, such as the provision on nondiscriminatory treatment of digital products, or providing an enabling framework for digital trade such as through provisions on the domestic electronic transaction legal framework, recognition of the legal validity of electronic signatures or electronic authentication methods, the acceptance of electronic documents as the legal equivalent of their paper versions, and open government data. The most interesting provision, though, is the provision on principles on access to and use of the internet for digital trade (USMCA Article 19.10). This clause is mainly designed to deal with the risks that market players who own or control key infrastructures could abuse their power by unreasonably denying their business users access to their infrastructures, making it impossible for these users to conduct e-commerce activities. To deal with this problem, the agreements provide consumers (including business users) with the freedom of access to the internet and to use it for e-commerce, subject only to network management and network safety restrictions. This provision apparently grew out of the net neutrality principle from the domestic telecom regulatory framework in the US. In a way, it supports digital companies' businesses in the economies in which they operate, so that they would not be held hostage by the network-throttling practices often found in some of the economies.

6.2.2 People's Republic of China

For the PRC, the key to data regulation is data security. Such a regulatory approach, dubbed "data regulation with Chinese characteristics" in Gao (2019),

[28] Text—S.1353—113th Congress (2013–2014): Cybersecurity Enhancement Act of 2014. 2013. https://www.congress.gov/bill/113th-congress/senate-bill/1353/text (accessed 15 June 2021).

[29] Sec. 101. Public–Private Collaboration on Cybersecurity.

is the result of an evolution spanning 25 years. The evolving approach closely traces the development of the internet sector in the PRC. In the early days of the internet, regulations focused on computer and internet hardware, requiring all connections to go through official gateways sanctioned by the government. As the internet gradually expanded with the proliferation of software and apps catered to popular uses, the government moved on to regulate the software and started to require software used for internet access to be sanctioned by the government. As cyberspace became an indispensable part of everyday life and began to permeate every sector from socializing, shopping, to entertainment and education, the government shifted focus to the regulation of content and now data, especially with the rise of big data and artificial intelligence. Moreover, data regulation has now been elevated to the level of national security with the introduction of the Cybersecurity Law in 2016. The agency responsible for content regulation, the Cyberspace Administration of China, mainly focuses on making sure that the cyberspace is secure.

At the international level, the PRC has traditionally taken a cautious approach to provisions on digital trade in trade agreements. Until recently, it did not even include e-commerce chapters in its regional trade agreements (RTAs). This changed only with its FTAs with the Republic of Korea and Australia, both signed in 2015. Nonetheless, the provisions in these two FTAs remain rather modest, as they mainly address issues related to trade facilitation, such as moratoriums on customs duties on electronic transmission, recognition of electronic authentication and electronic signature, protection of personal information in e-commerce, paperless trading, domestic legal frameworks governing electronic transactions, and the need to provide consumers using electronic commerce with protection on the same level as traditional forms of commerce.

A major breakthrough was made in the Regional Comprehensive Economic Partnership (RCEP) Agreement, which the PRC signed with other 14 economies in the region in November 2020. Under the chapter on e-commerce, the PRC and all other RCEP members agreed to not "require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory" (Article 12.14), or "prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person" (Article 12.15).[30]

Agreeing to the twin provisions on data flow and data localization under the RCEP is a notable evolution in the PRC's approach. In practice, it is important to keep in mind that both provisions are overshadowed by national security concerns allowing members to adopt "any measure that it considers necessary

[30] Association of Southeast Asian Nations (ASEAN) Secretariat. Legal Text of the RCEP Agreement. https://rcepsec.org/legal-text/.

for the protection of its essential security interests." Such security measures "shall not be disputed by other Parties," and will not be subject to legal challenge.[31]

Another exception to these two obligations is "any measure ... that [the implementing Party] considers necessary to achieve a legitimate public policy objective." The necessity test is not the one found in the general exceptions clause under GATT Art. XX, but is the one under the security exceptions clause under GATT Art. XXI—i.e., what the party taking such measure "considers necessary." This approach is further confirmed by the footnotes to the two provisions on data flow and data localization, which "affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party."

What then, could such "legitimate public policy objective" entail? Like most other economies, this could include laws for the protection of privacy or personal information. Yet, the PRC approach to privacy protection also comes with its own limitations. To start, privacy protection is a rather new concept in the PRC law. Privacy was first recognized as a civil right under the Tort Liability Law in 2009. This was duly incorporated into PRC's Civil Code enacted in 2020, which has a separate chapter on privacy and personal information protection as part of the volume on personality rights.[32] According to Art. 1035 of the Civil Code, the processing of personal information shall be based on the consent of the data subject, "except if there are different requirements under laws or administrative regulations," which envisages the cases where laws do not require the consent of the data subject.

In addition, government agencies in charge of cybersecurity monitoring and management and their staff are required to keep confidential any personal or privacy information they obtain in the discharge of their duty. The PRC's new Personal Information Protection Law also confirms that data processors do not need to obtain the consent of the data subject when discharging official duty and responsibility (Article 13.3) (Box 6.2).

At the same time, it should also be noted that many of these features are not unique to the PRC and are found in other privacy laws, such as the GDPR.[33]

[31] RCEP chapter on e-commerce is carved out from the normal dispute settlement procedure.

[32] Chapter 6, Volume 4 of The State Council of the PRC. See Civil Code of the People's Republic of China. http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.

[33] For example, Article 6 of the GDPR.

Box 6.2: The New Personal Information Protection Law of the People's Republic of China

The People's Republic of China (PRC) Personal Information Protection Law (PIPL) was adopted at the 13th National People's Congress on 20 August 2021 and took effect that November. The PIPL provides significant enhancement to the PRC's privacy protection regime. For example, besides the existing principles of lawfulness, fairness, and necessity, the new law adds a principle of good faith for the processing of personal information (Article 5). This is not just an abstract principle, but is reflected in the addition of new rules such as the prohibition of artificial intelligence powering differentiation pricing, a practice long complained by consumers (Article 24). The law also explicitly spells out specific consumer rights, such as the right to refuse to consent or to withdraw consent already given (Article 15), along with a corresponding provision banning data processors from refusing to provide products or services unless such consent is essential for such products or services (Article 16). The biggest impact of the law is on the big platform companies, which are subject to additional obligations such as the establishment of independent bodies composed of mainly outsiders to monitor their protection of personal information (Article 58). This is, in some ways, similar to the regulation of the "gatekeepers" under the European Union's proposed Digital Markets Act.[a] In addition, the provision on data portability could also constrain big platform companies' capacity to keep the consumers' data as their own and reduce their competitive advantage (Article 45). The new law echoes the PRC's commitments in the Regional Comprehensive Economic Partnership by explicitly allowing cross-border data transfer, as per commitments under international agreements (Article 38). This could open the door for further international collaboration such as the participation in the Asia-Pacific Economic Cooperation (APEC) cross-border privacy rules system.[b]

[a] Article 2, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en.

[b] APEC. What Is the Cross-Border Privacy Rules System? https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

Source: Author.

While it is common to have personal information protection laws as exceptions to the twin provisions on data flow and data localization, the exceptions under the PRC data regulation regime cover not only personal data and "important data," a highly important concept that is poorly defined (Gao 2021). In addition, the newly enacted Data Security Law adds another concept of "national core data." This is defined as "data-related to national security, the lifeline of the national economy, people's livelihood and major public interests" and will be subject to "a more stringent management system." It is likely that the scope of the new category of "national core data" will be narrower than "important data," but it is unclear how much narrower it will be.

6.2.3 European Union

The EU has, as its main concern, the privacy of the individual. This started with the Data Protection Directive in 1995, which prohibits the transfer of personal data to non-EU economies, unless they have privacy protection standards deemed adequate (Gao 2021). The directive was replaced by the GDPR in 2018 (Aaronson and Leblond 2018).

Despite having a name that suggests a broader reach, the GDPR applies only to personal data, which is defined as "any information relating to an identified or identifiable natural person ('data subject')" (Article 4.1). It regulates the behavior of the data controller and processor, which are respectively defined as the one who "determines the purposes and means of the processing of personal data" and "processes personal data on behalf of the controller" (Articles 4.7 and 4.8). Under the GDPR, the processing of personal data is only allowed with the "explicit" consent of the data subject and a few other specifically enumerated reasons (Articles 49.1.a and 6.1), under a set of principles that specifies the scope and manner of such processing (Mattoo and Meltzer 2018). Transfer of personal data to third economies is allowed only on the basis of an adequacy decision or appropriate safeguards (Articles 45 and 46).

Since its introduction, the GDPR has become the gold standard of privacy protection. Encouraged by its success, senior EU officials started to advocate for "technological sovereignty" (Burwell and Propp 2020; European Commission 2019b; Scott 2019). This concept is closely linked with "digital sovereignty," which was elaborated in the European Commission's "Communication on a European Strategy for Data" unveiled in February 2020 (European Commission 2020). Many commentators have pointed out that the new data strategy is designed to "counter the strong position of US and Chinese digital companies in the European market" (Burwell and Propp 2020) and remedy "the key European disadvantage" of "the lack of significant European digital corporations with global influence" (Hobbs 2020). The new data strategy aims to create "a single European data space" so that "by 2030, the EU share of the data economy—data stored, processed and put to valuable use in Europe—at least corresponds to its economic weight, not by *fiat* but by choice" (European Commission 2020).

This quest for digital sovereignty started out as a defensive move to fend off the encroachment into EU cyberspace by big firms from the outside. By combining the powers of its huge market and regulatory apparatus, the EU is trying to reclaim digital sovereignty, not only from other economies, but more importantly, from the digital giants.

The data strategy can be seen as part of a broader EU plan to establish "strategic autonomy." The concept started as an idea from a 1994 white paper on defense published by France (Government of France 1994). Gradually,

however, it was accepted by the big three member states: Germany, France, and Italy (Franke and Varma 2019). The concept was adopted by the European Union in 2016 when it unveiled its Global Strategy, which was supposed to "nurture[s] the ambition of strategic autonomy" (European Commission 2016). With the election of Donald Trump as US president and amid Brexit (the United Kingdom leaving the European Union), the concept started to take off among EU member states (Franke and Varma 2019). While there was some ambiguity on the exact content of the concept, the bigger member states typically perceived it as referring to decision-making autonomy (Franke and Varma 2019). This was recently validated in the February 2021 trade strategy paper, which refined it as a concept of "open strategic autonomy" emphasizing "the EU's ability to make its own choices and shape the world around it through leadership and engagement, reflecting its strategic interests and values," with a priority area being the digital agenda (European Economic and Social Committee 2021).

On data flow, the EU takes a bifurcated approach. Nonpersonal data are supposed to flow freely under its Framework for the Free Flow of Non-Personal Data,[34] while cross-border flows of personal data are subject to stringent requirements under the GDPR, despite its explicit recognition that "[f]lows of personal data to and from countries outside the Union and international organizations are necessary for the expansion of international trade and international cooperation."[35] Due to high compliance costs (as noted by Irwin 2021), however, the GDPR has proven to be "challenging especially for the small and medium-sized enterprises."[36] Schechner and Drozdiak (2018) report that to stay away from potential legal challenges, many US websites blocked access by EU customers before the GDPR went into effect, and these remained unavailable in the EU months after (South 2018).

In addition to its negative impact on cross-border data flow, the GDPR also creates pressure toward data localization, especially after the decision of the Court of Justice of the European Union in Data Protection Commissioner v. Facebook Ireland, Maximillian Schrems (Schrems II).[37] However, as Chander (2020) eloquently argues, data localization not only will not "solve the policy objectives identified in Schrems II, it will create "its own policy problems." The data localization requirements for nonpersonal data were banned by the Framework for

[34] Framework for the Free Flow of Non-Personal Data in the European Union of the European Parliament and of the Council of 14 November 2018, Regulation 2018/1807.

[35] GDPR, Recital 101.

[36] Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition—two years of application of the General Data Protection Regulation. SWD(2020) 115 final. Brussels. 24 June 2020.

[37] Case C-311/18, ECLI:EU:C:2020:559 (16 July 2020).

the Free Flow of Non-Personal Data, which mandated EU member states to repeal their data localization laws by 30 May 2021. In contrast, however, the GDPR does not include such a prohibition. On the contrary, data localization requirements for personal data are quite common among EU countries (Burwell and Propp 2020), with most covering special categories of sensitive data like health-related personal data or financial services data (Cory 2017). On the latter point, it is worth noting that the EU approach again diverges from the current US approach. When the US negotiated the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), it carved out the entire financial services sector from the scope of its e-commerce chapter, including prohibition of data localization requirements.[38] However, the new USMCA explicitly brought the financial services sector under the ban by stating that data localization should not be required "so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory."[39] It will be interesting to see whether the EU approach shifts closer to the US approach in the future.

In its RTAs, the EU has not been able to include substantive language on data issues until recently. This was due to the internal differences between the two director-generals (DGs) with overlapping jurisdictions on the issue, i.e., DG for Trade, which favors free trade for the sector, and DG for Justice, which has concerns over personal information protection (Aaronson 2019). Thus, notwithstanding its strong interest in privacy protection, the EU position in existing FTAs has been rather modest, which usually requires parties to adopt their own laws for personal data protection to help maintain consumer trust and confidence in electronic commerce.[40] In February 2018, however, the two DGs were finally able to reach a compromise, which included, on the one hand, horizontal clauses on free flow of all data and ban on localization requirements, while on the other, affirming the EU's right to regulate by making clear that it shall not be subject to investor–state arbitration.[41] Despite this development, the EU still seems to prefer handling data flow issues through bilateral "adequacy" recognitions, which so far have been granted to only a dozen countries.[42] In many of its latest FTAs,

[38] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Art. 14.1.

[39] USMCA, Art. 17.18.2.

[40] USMCA, Art. 17.18.2.

[41] USMCA, Art. 17.18.2, at 262.

[42] So far, the EU has granted adequacy recognitions to Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay. See European Commission. Adequacy Decisions. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

data flow issues were left out in the main text, with a separate adequacy decision adopted. An example is its Economic Partnership Agreement (EPA) with Japan (European Commission 2019a). In that case, the adequacy decision was adopted separately from the EPA, which does not include commitments on free flow of data.[43] The recent FTA with Viet Nam lacks not only provisions on data flow and localization, but also any plan for an adequacy decision.

6.2.4 Why the Differences?

The diverging approaches among the three major players are not randomly chosen. Instead, they reflect deeper differences in their respective commercial interests and regulatory approaches within each jurisdiction.

First, the global e-commerce market is largely dominated by the PRC and the US. Among the 10 biggest digital trade firms in the world, six are American and four are Chinese.[44] Of course, this does not necessarily mean that they must share the same position. Upon closer examination, one can see that US firms on the list tend to be pure digital services firms. Firms like Facebook, Google, and Netflix do not sell physical products, but only provide digitalized services such as online search, social network, or content services. In contrast, two of the top three Chinese firms—Alibaba and JD.com—sell mainly physical goods. This is why the US focuses on the "digital" side, while the PRC focuses on the traditional "trade" side when it comes to digital trade, as the author has argued in another paper (Gao 2018).

It can be said that the PRC also has giant pure digital firms like Baidu and Tencent, which are often referred to as the Google and the Facebook of the PRC. However, because they serve the domestic market almost exclusively and most of their facilities and operations are based in the PRC, they do not share the demands for free cross-border data flow as their US counterparts, which have data centers in strategic locations around the world.

As for the EU, with no major players in the game, some view their restrictive privacy rules as a form of "digital protectionism" to fend off the invasion of American and Chinese firms (Aaronson 2019).

The second influence is their different domestic regulatory approaches. In the US, the development of the sector has long benefited from its "permissive legal framework" (Chander 2013), which aims to reduce government regulation

[43] According to Art. 8.81 of the EPA, "The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement."

[44] Wikipedia. List of Largest Internet Companies. https://en.wikipedia.org/wiki/List_of_largest_internet_companies (accessed 20 February 2020).

of the internet to a minimum and relies heavily on self-regulation in the sector. Such policy is even codified in the law, with the Telecommunication Act of 1996 explicitly stating that it is "the policy of the United States ... to preserve the vibrant and competitive free market that presently exists for the internet and other interactive computer services, unfettered by Federal or State regulation."[45] Therefore, it is no surprise that the US wishes to push for deregulation and the free flow of information at the international level, a long-standing policy that can be traced back to the Framework for Global Electronic Commerce announced by the Clinton administration in 1997 (Aaronson and Leblond 2018). At the same time, the US does not have a comprehensive privacy protection framework. Instead, it relies on a patchwork of sector-specific laws, which provides privacy protection for consumers of a variety of sectors such as credit reports and video rental (Chander 2013). This is complemented by case-by-case enforcement actions by the Federal Trade Commission, and self-regulation by firms themselves. This explains why, in its RTAs, the US does not mandate uniform rules on personal information protection but allows members to adopt their own domestic laws.

On the other hand, in the PRC, the internet has been subject to substantial government regulations, which not only dictate the hardware one must use to connect to international networks, but also the content that may be transmitted online (Gao 2019). Many foreign websites are either filtered or blocked in the PRC, which confirms its cautious position on free flow of data. Moreover, in 2017, the PRC also adopted the Cybersecurity Law, which requires operators of critical information infrastructure to store locally personal information they collected or generated in the PRC. Privacy protection is also weak in the PRC, as it was only incorporated into its legal system in 2009, along with exemptions for the government.

The EU, in contrast, has a long tradition of human rights protection, partly in response to the atrocities of World War II (Mattoo and Meltzer 2018). Coupled with the absence of major digital players wielding significant market power and the lack of a strong central government with overriding security concerns, this translates into a strong emphasis on privacy in the digital sphere. Moreover, the EU is also able to transcend the narrow mercantilist confines of the US (Schwartz and Peifer 2017), and recognize privacy not only as a consumer right, but also as a fundamental human right that is recognized in several fundamental EU instruments[46] and the constitutions of many member states.[47] Such a refreshing

[45] Telecommunication Act of 1996, 47 U.S.C. 230(b)(2). https://www.law.cornell.edu/uscode/text/47/230 (accessed 20 April 2018).

[46] For example, Art. 8 of the 8 Charter of Fundamental Rights of the European Union, 2000 O.J C 364/10; Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 312 U.N.T.S. 222, Art. 8.

[47] These include Germany, Greece, Hungary, Poland, and Spain (Matto and Meltzer 2018).

perspective is probably the biggest contribution that the EU has made to digital trade issues.

6.3 Trade Agreements in Developing Asia

The three models discussed in this chapter are not limited to the three jurisdictions. Instead, as illustrated by Ferracane and van der Marel (2021) in their recent comprehensive survey, these three models cover most of the economies around the world, including Asia and the Pacific.

To assess the state of play in Asia and the Pacific, this chapter maps the main agreements in the region. More specifically, the mapping covers all FTAs by the main players in the region with chapters on e-commerce or digital trade since 2000. The mapping also covers the mega-FTAs in Asia and the Pacific, i.e., the RCEP, CPTPP, USMCA, and the EU–Canada Comprehensive Economic and Trade Agreement, as well as the two stand-alone digital trade agreements: the Digital Economy Partnership Agreement and digital economy agreements. Using the CPTPP and USMCA as a benchmark, the mapping groups digital trade provisions in these trade agreements into four categories.

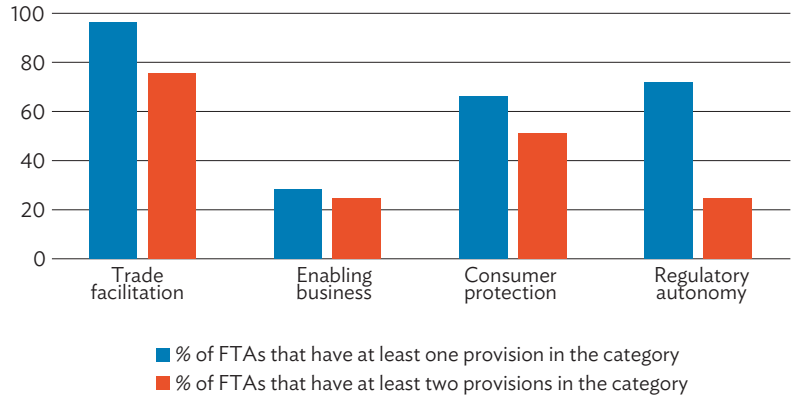
The components of the first category are the six provisions designed to create a facilitating environment for digital trade in general, such as the provisions on the elimination of customs duties on electronic transmission, nondiscriminatory treatment of digital product, domestic electronic transactions framework, electronic authentication and electronic signatures, and paperless trading provisions. These provisions provide the necessary regulatory and technological environment to enable the smooth functioning of digital trade, which also forms the bedrock for conducting digital services trade.

The second category consists of five provisions to minimize the commercial and regulatory burden for digital services trade providers, such as those on access to and use of the internet for electronic commerce, free flow of data, prohibition of data localization requirements, prohibition on forced transfer of source code, and open government data. These provisions focus on the most common regulatory and commercial obstacles facing digital services trade firms. By removing these obstacles, digital services will be able to flow more freely across economies, creating massive economies of scale with the data they amass across different markets.

The third category includes three provisions to protect the interests of consumers, such as those on online consumer protection, privacy and personal information protection, and unsolicited commercial electronic messages. By addressing the main concerns of consumers, these provisions enhance the trust of consumers in digital services trade and so indirectly boost the rate of take-up of digital services among consumers.

The last category includes four provisions to preserve the regulatory autonomy of the government, such as those on cybersecurity, exceptions, and cooperation. These provisions help governments to reserve the space necessary to deal with various social policy objectives even though they might ostensibly be inconsistent with various obligations under the digital trade chapter.

Figure 6.1: Free Trade Agreements with at Least One Provision in Each Category



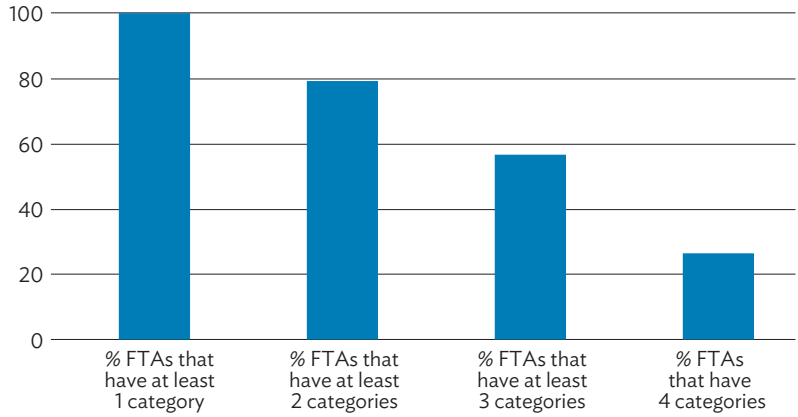
FTA = free trade agreement.

Source: Author's calculations.

Among the four types of provisions, the first is the most popular, with more than three-quarters of the surveyed FTAs including at least two provisions in this category (Figure 6.1). There are several possible reasons for this. The first is that many of these obligations are not entirely new, but repeats obligations in other international agreements, such as the UNCITRAL Model Law on Electronic Commerce (1996), the United Nations Convention on the Use of Electronic Communications in International Contracts, and the WTO Trade Facilitation Agreement. Moreover, as these provisions lay down the infrastructure necessary to facilitate digital trade and do not prescribe a specific regulatory approach

on sensitive issues, they face the least resistance from the bureaucracy and governments generally welcome them. At the same time, even as these provisions can help developing economies foster trade in digital services, there could be problems in implementation. The first is that implementation of some provisions might require additional investment in hardware and software, which can be a challenge for some developing economies. Second, merely having the facilities might not be sufficient. Instead, the statutory requirements on documentary formalities might also need to be modified to account for the new ways of contracting and approval. As many developing economies lack the experience and expertise in this regard, they might need technical assistance from the relevant international agencies.

Figure 6.2: Free Trade Agreements with Provisions in at Least One to All Categories



FTA = free trade agreement.

Source: Author's calculations.

The second type of provision does facilitate digital services trade by taking down regulatory barriers that blocks or impedes trade flow. The problem, however, is that the primary beneficiaries of such measures tend to be overseas firms, which supply their services through the cross-border supply mode. This could raise a host of economic and social issues, such as crowding out domestic services suppliers and therefore taking away both sales and jobs, reduction of government revenues as the overseas services suppliers are unlikely to pay value-added taxes or income tax, suppressing the development of the local e-commerce suppliers,

and raising the hurdles for regulatory enforcement actions as the online suppliers are much more difficult to regulate. Because of these issues, many developing economies are reluctant to agree to these provisions, which are included in only a quarter of surveyed FTAs (Figure 6.1). Again, here the issue is not just purely economic, the lack of regulatory capacity is also a major issue that regulators in many economies have to grapple with. On the other hand, without these policies, the digital giants would hesitate to enter the local market due to cybersecurity concerns (when data cannot flow freely) and additional costs (for building local servers). Thus, many developing economies also understand the need to agree to these provisions, at least as a welcoming signal to foreign digital firms. Two things need to be done to assuage the concerns of these developing economies. The first is to raise awareness on the basics of digital trade, especially those of data transfer, so that it is understood that even localization requirements might not entirely prevent many of the potential problems associated with the free flow of data. The second would be to help developing economies learn from the regulatory practices in other economies. One such example could be the practices that can operate at sufficient regulatory capacity even with the offshore storage of data, provided they have "immediate, direct, complete, and ongoing access to" such data (USMCA Art. 17.18).

The third type of provision does not directly contribute to the development of digital services trade. But by fostering a trustworthy environment for the consumers, they may also make indirect contributions to digital trade by easing the concerns of the consumers against digital trade. The problem, however, is that developing economies often lack domestic laws and regulations on many of the issues in this category to start with. This makes it harder for them to formulate relevant laws and regulations, and sometimes such regulations are implemented in a way that affects digital suppliers more than traditional suppliers, which could raise national treatment issues as traditional suppliers are typically domestic suppliers. This is also reflected in Figure 6.1, with only half of the surveyed FTAs including at least two provisions from this category. Again, technical assistance would greatly help developing economies as they enter this new regulatory field.

The fourth type of provision, by design, boosts the power of the government vis-a-vis the digital firms and so does not appear to be facilitative in nature. These provisions provide the government the maneuvering space necessary to keep digital services under tighter regulatory supervision, which is crucial for many developing economies, with the bulk of digital services trade being provided by foreign suppliers. This also explains the popularity of these provisions, with more than 70% of the surveyed FTAs including at least one provision in this category (Figure 6.1), and even more if general exceptions clauses in the other chapters are included. Overall, 26% of the surveyed FTAs include provisions in each of the four categories (Figure 6.2).

To foster the development of the sector, developing Asia will need to beef up the provisions in the second and third categories. Given the complexity of digital services trade, it would be unrealistic to assume that the mere inclusion of these provisions would boost trade levels. Instead, this needs to be coupled with other efforts, such as building up the necessary infrastructure for digital trade, and putting in place the appropriate regulatory environment to strike the right balance between risk control and market liberalization. Given that many of these economies do not have sufficient experience, it is probably a good idea to start with market liberalization at the regional level. This could be facilitated by mutual recognition agreements on services, which so far has been restricted to the rich economies. Economies with similar regulatory frameworks can develop such recognition arrangements at the bilateral and regional levels first, before expanding them to a wider level.

Bibliography

Aaronson, S. A. 2019. What Are We Talking about When We Talk about Digital Protectionism? *World Trade Review*. 18. pp. 541–577.

Aaronson, S. A., and P. Leblond. 2018. Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO. *Journal of International Economic Law*. 21 (2). pp. 245–72. https://doi.org/10.1093/jiel/jgy019.

Burwell, F., and K. Propp. 2020. The European Union and the Search for Digital Sovereignty: Building 'Fortress Europe' or Preparing for a New World? *Research Reports*. June. Washington, DC: Atlantic Council.

Chaisse, J., H. Gao, and C. Lo, eds. 2017. *Paradigm Shift in International Economic Law Rule-Making: TPP as a New Model for Trade Agreements*. Singapore: Springer.

Chander, A. 2013. *The Electronic Silk Road: How the Web Binds the World Together in Commerce*. New Haven, CT: Yale University Press.

———. 2020. Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*. 23 (3). pp. 771–784.

Cory, N. 2017. Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? May. Information Technology & Innovation Foundation. http://www2.itif.org/2017-cross-border-data-flows.pdf.

Delimatsis, P. 2012. The Puzzling Interaction of Trade and Public Morals in the Digital Era. In M. Burri and T. Cottier, eds. *Trade Governance in the Digital Age: World Trade Forum*. Cambridge: Cambridge University Press.

European Commission. 2016. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. Brussels.

———. 2019a. European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows. *Press Corner*. 23 January. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.

———. 2019b. Questions to the Commissioner-Designate Thierry Breton. https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf.

———. 2020. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 19 February. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

European Economic and Social Committee. 2021. *Trade Policy Review—An Open, Sustainable and Assertive Trade Policy*. https://trade.ec.europa.eu/doclib/html/159438.htm.

Ferracane, M. F., and E. van der Marel. 2021. Regulating Personal Data: Data Models and Digital Services Trade. *Policy Research Working Paper*. 9596. Washington, DC: World Bank.

Franke, U., and T. Varma. 2019. Independence Play: Europe's Pursuit of Strategic Autonomy. *European Council on Foreign Relations*. 18 July. https://ecfr.eu/special/independence_play_europes_pursuit_of_strategic_autonomy/.

Gao, H. 2008. Commentary on Telecommunication Services. In R. Wolfrum and P.-T. Stoll, eds. *Max Planck Commentaries on World Trade Law*. Volume VI: WTO—Trade in Services. Leiden: Brill Publishers.

———. 2012. Googling for the Trade-Human Rights Nexus in China: Can the WTO Help? In M. Burri and T. Cottier, eds. *Trade Governance in the Digital Age: World Trade Forum*. Cambridge: Cambridge University Press.

———. 2017. The Regulation of Digital Trade in the TPP: New Trade Rules for the Digital Age. In J. Chaisse, H. Gao, and C. Lo, eds. *Paradigm Shift in International Economic Law Rule-Making: TPP as a New Model for Trade Agreements*. Singapore: Springer.

———. 2018. Digital or Trade? The Contrasting Approaches of China and US to Digital Trade. *Journal of International Economic Law*. 21 (2). June. pp. 297–321.

———. 2019. Data Regulation with Chinese Characteristics. *SMU Centre for AI & Data Governance Research Paper*. No. 2019/04. Singapore: Singapore Management University.

———. 2021. Data Regulation with Chinese Characteristics. In M. Burri, ed. *Big Data and Global Trade Law*. Cambridge: Cambridge University Press.

Government of France. 1994. Livre Blanc sur la Défense 1994 (1994 White Paper on Defense). http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le-livre-blanc-sur-la-defense-1994.pdf.

Greenleaf, G. 2018. *The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on 'the Right to Privacy in the Digital Age' to the UN*

High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. 8 April. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf.

Hobbs, C. 2020. Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry. 30 July. European Council on Foreign Relations. https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

Irwin, L. 2021. How Much Does GDPR Compliance Cost in 2021? IT Governance European Blog. June. https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020.

Kariyawasam, R. 2012. Better Regulation of Digital Markets: A New Look at the Reference Paper. In M. Burri and T. Cottier, eds. *Trade Governance in the Digital Age: World Trade Forum*. Cambridge: Cambridge University Press.

Mattoo, A., and J. P. Meltzer. 2018. International Data Flows and Privacy: The Conflict and Its Resolution. *Journal of International Economic Law*. 21 (4). pp. 769–789.

Peng, S. Y. 2016. GATS and the Over-the-Top Services: A Legal Outlook. *Journal of World Trade*. 50 (1). pp. 21–46.

Raghavan, C. 2000. To Cluster or Not to Cluster (in GATS). *South-North Development Monitor*. 19 July. Pulau Pinang, Malaysia: Third World Network .

Schechner, S., and N. Drozdiak. 2018. U.S. Websites Go Dark in Europe as GDPR Data Rules Kick In. *Wall Street Journal*. 25 May 2018. https://www.wsj.com/articles/u-s-websites-go-dark-in-europe-as-gdpr-data-rules-kick-in-1527242038.

Schwartz, P. M., and K. N. Peifer. 2017. Transatlantic Data Privacy Law. *The Georgetown Law Journal*. 106 (115). pp. 117–179.

Scott, M. 2019. What's Driving Europe's New Aggressive Stance on Tech? *Politico*. 28 October. https://www.politico.com/news/2019/10/28/europe-technology-silicon-valley-059988.

South, J. 2018. More than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months after GDPR Took Effect. *NiemanLab*. 7 August. https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.

Tuthill, L., and M. Roy. 2012. GATS Classification Issues for Information and Communication Technology Services. In M. Burri and T. Cottier, eds. *Trade Governance in the Digital Age: World Trade Forum*. Cambridge: Cambridge University Press.

United States International Trade Commission (USITC). 1998. *US Schedule of Commitments under the General Agreement on Trade in Services (with explanatory materials prepared by the USITC, includes supplemental commitments and MFN exemptions on basic telecommunication services, finalized on 15 February 1997,*

and on financial services, finalized 13 December 1997). Investigation No. 332–354. August.

World Trade Organization (WTO). 1991. *Services Sectoral Classification List*. MTN. GNS/W/120. 10 July. Geneva.

———. 1994. *United States of America, Schedule of Specific Commitments*. GATS/SC/90. 15 April. Geneva.

———. 1996. *Negotiating Group on Basic Telecommunications, Telecommunications Services: Reference Paper*. 24 April. Geneva.

———. 1998. *Work Programme on Electronic Commerce (Adopted by the General Council on 25 September 1998)*. WT/L/274. 30 September. Geneva.

———. 1999. *Work Program on Electronic Commerce: Progress Report to the General Council (Adopted by the Council for Trade in Services on 19 July 1999)*. S/L/74. 27 July. Geneva.

———. 2000a. *Council for Trade in Services Special Session: Communication from the European Communities and Their Member States—The Cluster Approach*. S/CSS/W/3. 22 May. Geneva.

———. 2000b. *Council for Trade in Services Special Session: Communication from the United States—Framework for Negotiation*. S/CSS/W/4. 13 July. Geneva.

———. 2001. *Guidelines for the Scheduling of Specific Commitments under the GATS, Adopted by the Council for Trade in Services on 23 March 2001.* S/L/92. 28 March.

———. 2005. *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (Report of the Appellate Body). WT/DS285/R. 7 April.

———. 2010. *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (Report of the Appellate Body)*. WT/DS363/AB/R. 19 January. Geneva.

———. 2013. *Work Programme on Electronic Commerce, Dedicated Discussion on Electronic Commerce Under the Auspices of the General Council: Report to the 21 November 2013 Meeting of the General Council*. WT/GC/W/676. 11 November. Geneva.

———. General Agreement on Trade in Services. https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm.

———. MC12 Briefing Note: E-commerce. https://www.wto.org/english/thewto_e/minist_e/mc12_e/briefing_notes_e/bfecom_e.htm#.YwyWcHYykv8 (accessed 30 August 2022).

Wunsch-Vincent, S., and A. Hold. 2012. Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Negotiations. In M. Burri and T. Cottier, eds. *Trade Governance in the Digital Age: World Trade Forum*. Cambridge: Cambridge University Press.