SECTION

4

The ways forward

Chapter 15

Data regulation in trade agreements: different models and options ahead

Henry Gao*

** The contents of this chapter are the sole responsibility of the author and are not meant to represent the position or opinions of the WTO or its members.*

Introduction

"Data is the new oil". Just like oil, which powered the economy in the last century, data are what moves the world today. This is especially true for international trade. The crucial role played by data can be observed at every step of the process, from the conception of a new product and the sourcing of raw materials and parts, to the manufacturing process and the transportation of products across borders, until they finally reach the hands of consumers from every corner of the world.

To be sure, the process of international trade has always been accompanied by the exchange of data, be it about the product, the seller or the buyer. What is unprecedented, though, is the ubiquity of data in the modern economy. This is a manifestation of the many important changes that emerged in the first two decades of the new century. For trade in goods, these include the following factors: the emergence of regional and even global supply chains, which involves the sharing and exchange of data among many parts manufacturers during the various stages leading to the final products; the invention of 3D printing, which makes it easy to customize products based on the needs of customers and blurs the boundary between the manufacturer and the consumer; and the Internet of Things, which turns traditional products into conduits for the collection, analysis and utilization of data. Similar changes can also be observed in the realm of services trade, where the advent of the internet has not only removed the natural barrier of physical distance and made many hereto non-tradable services tradable, but also, through the servicification of goods (Lanz and Maurer, 2015; WTO, 2018, pp. 111-116 and 157), rendered the movements of physical goods unnecessary and turned them into new categories of services trade.

More importantly, rather than acquiring the goods or services for their sole use, consumers nowadays often find that all they get is the temporary right to access and deploy data. At the same time, as the access to data is democratized, the amount of data generated by users also grows exponentially. A report by McKinsey, for example, estimated that global data flow has grown 45 times in the decade from 2005 to 2014 (Manyika et al., 2015). Such phenomenal growth also led to breakthroughs in artificial intelligence, where powerful machine learning helped to unleash the full potential of big data to generate refreshing insights into everything it touches. In the area of trade, for example, big data not only helps us to gain more comprehensive and accurate information about the shifts in demand and supply so that manufacturers may better adjust their productions, but also churns out more refined granular analysis about

"Rather than acquiring the goods or services for their sole use, consumers nowadays often find that all they get is the temporary right to access and deploy data."

the crucial differences between different segments in the market so as to better tailor the same product into many variations to cater to the individual needs of consumers.

National regulations

Given the growing importance of data in business and trade, more and more firms are trying to gather as much data as possible in this new gold rush. Due to the network effects (OECD, 2017, p. 135), the electronic commerce industry is, more often than not, a winner-takes-all game. This means that data is increasingly being concentrated into the hands of a few e-commerce giants such as Amazon, Facebook and Google. Such concentration of power leads to concerns over potential abuse, which in turn heightens the need to regulate the flow and transfer of data, both within and across national borders.

Any framework for data regulation would involve three groups of players: the individual, who provides the raw data, and uses the processed data; the firm, which processes the 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, while 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 European Union, which recognizes "[t]he protection of natural persons in relation to the processing of personal data" as "a fundamental right".[1] On the other hand, some jurisdictions put the commercial interests of firms first. In the United States, this is reflected in the 1996 Telecommunication Act, which notes that it is "the policy of the United States … to preserve … free market …unfettered by Federal or State regulation".[2] In contrast, national security concerns are often cited to justify restrictions on cross-border data flows, albeit in varying degrees in different countries. A recent example is China's 2017 Cybersecurity Law, which imposed several restrictions aiming to "safeguard cyber security, protect cyberspace sovereignty and national security".[3]

Traditionally, restrictions on cross-border data flow were the most common type of digital protectionism (Wu, 2017, pp. 22-23). More recently, however, data localization requirements have also become popular, with the following as main variations (Gao, 2018a, pp. 303-304):

1. Local commercial presence or residency requirements. The origin for such requirements can be traced back to the General Agreement on Trade in Services (GATS), where service providers are often required to have a local commercial presence before they can provide a service. While such requirements could potentially affect all service sectors, e-commerce is especially vulnerable as it is often detached from traditional brick-and-mortar establishments.

2. Local infrastructure requirements. These include both hardware requirements for service providers to use computing facilities located in the host territory and software requirements to use computer processing and/or storage services located in such territory.

3. Local content requirements. Depending on the *modus operandi* of the local content requirements, this obligation can be further divided into two categories. One is granting preferences or advantages to goods or electronically transmitted contents produced in a territory, or to local computing facilities or computer processing or storage services supplied locally. The other is requiring foreign service suppliers to purchase or use local goods or electronically transmitted contents.

4. Local technology requirements. This can also be broken down into two types of obligations. The first is the requirement for foreign service suppliers to transfer technologies as a condition of providing a service. This is often tied to the requirement to have a local partner. The other is the requirement for foreign service suppliers to purchase or use local technologies.

While data flow restrictions and data localization requirements are both barriers to e-commerce, it is important to note the differences between the two. Data flow restrictions curb the cross-border transfer of data. This normally targets the outflow, but can also affect the inflow, such as banning certain websites. As the restriction normally affects both domestic and foreign firms alike, it is more akin to a most-favoured nation (MFN) treatment type of restriction. While such restrictions make it more difficult for firms to move data around, it could reduce data breach risks for individuals and regulatory costs for states. On the other hand, data localization requirements tend to affect mostly foreign firms so they are more of a National Treatment issue. Such requirements obviously would increase costs for foreign firms, but they could also increase risks of personal data breach and even regulatory costs for states due to the duplication of data on both local and off-shore servers.

Emerging approaches

E-commerce has been featured in the World Trade Organization (WTO) negotiating agenda since 1998, when the members adopted the Declaration on Global Electronic Commerce,[4] which also established a temporary moratorium on customs duties on digital transmission. Pursuant to the Declaration, the General Council adopted the Work Programme on Electronic Commerce,[5] which divided up the work among several WTO bodies such as the Council for Trade in Services, the Council for Trade in Goods, the Council for Trade-Related Aspects of Intellectual Property Rights and the Committee on Trade and Development. However, notwithstanding its ambitious agenda, the Work Programme has so far languished along with the rest of the Doha Round. This changed only very recently, when renewed interests among the membership led to the launch of the Joint Statement Initiative on E-commerce on 25 January 2019.[6]

Even absent new rules, however, some of the existing rules in the WTO can still be expanded to cover e-commerce.

To the extent that e-commerce affects trade in goods, such rules could include the existing MFN and National Treatment rules in the General Agreement on Tariffs and Trade 1994 (GATT 1994), as well as the prohibition of local content requirements under the Agreement on Trade-Related Investment Measures (TRIMs). As most e-commerce activities do not involve tangible products, however, it seems that the GATS is more promising. For example, as mentioned earlier, data flow restrictions and data localization requirements could potentially be subject to GATS MFN and National Treatment obligations. Moreover, to the extent that data regulations are part of the specific commitments undertaken by a WTO member, they would be subject to the domestic regulation obligations under Article VI of the GATS, such as the requirements for the rules to be based on objective and transparent criteria, not more burdensome than necessary, and administered in a reasonable, objective and impartial manner. Given the close relationship between the internet and telecommunication, one may also argue for the application of the existing GATS disciplines on the telecom sector (Gao, 2011), such as the GATS Telecom Annex and the Telcom Reference Paper.

"Even absent new rules, some of the existing rules in the WTO can still be expanded to cover e-commerce."

In contrast to the slow progress in the WTO, many regional trade agreements (RTAs) have been able to include new rules on data regulations (Wu, 2017). The three main players in this regard are the United States, the European Union and China, with each having its own model.

1. The US model

As the world leader in digital trade, the United States has included rules on data regulation in many of its free trade agreements (FTAs), with the now-defunct Trans-Pacific Partnership (TPP) Agreement and the recently concluded United States-Mexico-Canada Agreement (USMCA) as leading examples.[7] The obligations in the two agreements can be divided into the following categories:

The first are passive obligations, which prohibit the members from adopting various protectionist policies such as customs duties on electronic transmission, discrimination against foreign digital products, restrictions on cross-border transfer of information, forced localization requirements and forced transfer of source codes. The provisions are designed to minimize the distortions created by government interventions and leave the development of the e-commerce market in the hands of the e-commerce players.

The second type are enabling provisions, which require member governments to introduce or maintain regulatory frameworks that facilitate the development of e-commerce. These include, for example, the requirements for the members to adopt domestic laws in line with the principles of the United Nations Commission on

International Trade Law (UNCITRAL) Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts, the recognition of the legal validity of electronic signatures or electronic authentication methods, and the acceptance of electronic documents as the legal equivalent of their paper versions. These provisions all deal with one key issue facing the e-commerce sector, i.e. the recognition of e-commerce transactions as equivalents of the traditional pre-internet ones.

In addition, recognizing the huge market power of the big digital players, the two agreements also include rules to check corporate power. First, market players that 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 address this problem, the agreements provide consumers (including business users) with the freedom of access to and use of the internet for e-commerce, subject only to network management and network safety restrictions. Second, to deal with potential misuse of consumer information, the agreements also include provisions on online consumer protection, personal information protection and unsolicited commercial electronic messages.

Recognizing the special needs of governments, both agreements have excluded government procurement and information held or processed by the government from the coverage of the digital trade chapters. Both also carved out the financial services sector, except that the USMCA provides that the prohibition on data localization requirements would continue to apply to the sector so long as a financial regulator has access to the relevant data for regulatory purposes. Both agreements also include language to cooperate on cybersecurity matters, with the USMCA going one step further by calling for risk-based regulations.

As the main proponent of the plurilateral Trade in Services Agreement (TISA) negotiations, the United States also proposed similar provisions in the draft TISA agreement. Most of these can be found in the e-commerce chapter, where the United States called for provisions that guarantee service suppliers the freedom to transfer information across countries for the conduct of their business; freedom for network users to access and use services and applications of their choice online, and to connect their choice of devices; prohibition of data localization requirements as a condition of supplying a service or investing; and prohibition of discrimination against electronic authentication and electronic signatures. In addition, the horizontal provisions also include prohibitions on a host of localization requirements as mentioned earlier. While they apply to all service sectors, they would be of particular relevance to e-commerce due to the nature of the sector.

2. The EU model

The main concern of the European Union, when it comes to e-commerce, is privacy protection. This is demonstrated by the GDPR, which recognizes privacy as not only a consumer right, but also a fundamental human right. The GDPR provides that

prior authorization is required before personal data can be transferred to a third country, unless that country is recognized by the European Union as providing an equivalent level of data protection.

However, in its RTAs, the European Union has not been able to include substantive language on such issues. This is due to the internal differences between the two Directors-General (DGs) with overlapping jurisdictions on the issue, i.e. DG-Trade, which favours free trade for the sector, and DG-Justice, which has concerns over personal information protection (Aaronson and Leblond, 2018, pp. 261-262). Thus, notwithstanding its strong interest in privacy protection, the EU positions in its existing FTAs have 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. In February 2018, however, the two DGs were finally able to reach a compromise position, which includes, on the one hand, horizontal clauses on the free flow of all data and a ban on localization requirements, while, on the other hand, affirming the European Union's right to regulate in the sector by making clear that it shall not be subject to investor-state arbitration.[8] Given the potentially intrusive rules in the GDPR, we might start to see a more aggressive push for stronger language on personal data protection in the European Union's RTAs in the future.

3. The China model

In contrast with the European Union and the United States, China has traditionally taken a cautious approach to data regulation in trade agreements. Until very recently, it has not even included e-commerce chapters in its RTAs.[9] This only changed with its FTAs with Australia and Korea, which were both signed in 2015. Moreover, the provisions in these two FTAs are rather modest, as they mainly address trade facilitation-related issues, such as a moratorium 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 a level of protection equivalent to that in traditional forms of commerce.

4. Reasons for 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.

First, the global e-commerce market is mostly dominated by China and the United States. Among the ten biggest digital trade firms in the world, six are American and four are Chinese.[10] Of course, this does not necessarily mean that they must share the same position. Upon closer examination, one can see that the US firms on the list tend to be pure digital service 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 United States focuses on digital

services while China focuses on traditional trade in goods enabled by the internet.

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

As for the European Union, with no major players in the game, their draconian privacy rules could be viewed as a form of digital protectionism (Aaronson, 2019) to fend off the invasions of American and Chinese firms into Europe.

The second influence is their different domestic regulatory approaches. In the United States, the development of the sector has long benefited from its "permissive legal framework", which aims to minimize government regulation on the internet 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". Therefore, it is no surprise that the United States wishes to push for deregulation and the free flow of information at the international level. At the same time, the United States 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. This is further complemented by case-by-case enforcement actions by the Federal Trade Commission (FTC), and self-regulation by firms themselves. This explains why, in its RTAs, the United States does not mandate uniform rules on personal information protection but allows members to adopt their own domestic laws.

On the other hand, in China, the internet has always been subject to heavy 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.[11] Many foreign websites are either filtered or blocked in China, which confirms China's cautious position on free flow of data. Moreover, in 2017, China also adopted the Cybersecurity Law, which requires the operators of critical information infrastructure to store locally personal information they collected or generated in China. This is at odds with the US demand to prohibit data localization requirements. Privacy protection is also weak in China, as it was only incorporated into the Chinese legal system in 2009, along with extensive exemptions for the government.

The European Union, in contrast, has a long tradition of human rights protection, partly in response to the atrocities of the Second World War. 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 European Union is also able to transcend the narrow mercantilist confines of the United States, and recognize privacy as not only a consumer right, but also a fundamental human right. Such a refreshing perspective is probably the biggest contribution made by the European Union to digital trade issues.

Elements for the way forward

With the revival of e-commerce discussions in the WTO in 2016, many members have made new submissions. Most of these largely reiterate their existing positions in RTAs and other plurilateral agreements. For example, in its July 2016 "non-paper", the United States called for the dismantling of both cross-border and domestic barriers to digital trade such as restrictions on cross-border data flow and government regulations requiring localization or forced transfer of technology or source code, and urged e-commerce firms to be given more autonomy including the freedom to use the technology, authentication methods, encryption methods, and facilities and services of their own choice. The Chinese submission in November 2016, on the other hand, focused more on trade facilitation measures such as simplified border measures and customs clearance, paperless trade and single window, and the establishment of platforms for cross-border e-commerce transactions such as the electronic World Trade Platform (eWTP), an idea first proposed by Alibaba Chairman Jack Ma. These positions have largely been carried over in their submissions in the Joint Statement Initiatives, which as of 10 February 2020 has received 52 submissions from the 77 participants.[12] We can gather the following from these submissions:

First, most developed countries and some developing countries seem to agree on the need to ensure free cross-border data flow in principle. At the same time, such freedom is often reserved for provision of covered services or investment only, and has been subject to exceptions on grounds ranging from personal information protection to the special needs of specific sectors like financial services. Some developing countries are more hesitant on the issue, due to either security or revenue concerns.

"Almost all countries agree with the goal of privacy or personal information protection, but they differ on how to get there."

Second, almost all countries agree with the goal of privacy or personal information protection, but they differ on how to get . there. While many countries are content with each country adopting its own domestic laws that meet certain minimum standards, privacy regimes with strong extraterritorial elements like the GDPR could create pressure for affected trade partners to adopt similar or even uniform rules.

Third, prohibition on data localization requirements is also widely accepted among more advanced economies, subject to carve-outs for government

data, government procurement, financial services, privacy protection and security measures. While some countries are considering data localization requirements in the false hope that such measures could create more local jobs or nurture local digital champions, more and more countries are coming to the realization that such measures would be more likely to harm rather than help the development of their digital sectors.

Given the uneven development of the sector in different countries, the most promising way forward would be to adopt a negotiation structure similar to the Trade Facilitation Agreement (TFA), with tiered obligations corresponding to the individual level of development of different members. At the core, there should be a set of commonly accepted minimum standards or basic principles, probably along the lines of the highly successful example of the Telecom Reference Paper. To enhance the participation of developing countries, there should also be technical assistance provisions to help developing countries progressively undertake more and more obligations. A major part of the technical assistance activities would undoubtedly be devoted to building the technological capacities by equipping them with the necessary hardware and software, but there should also be regulatory assistance projects as many developing countries lack the necessary regulatory experience with the sector.

In terms of the substantive content, such an agreement shall include the following elements: freedom of data flow for the provision of covered services, investments and intellectual property rights; prohibition of data localization requirements relating to the hardware, software or location of data storage, with narrowly defined exceptions for measures to protect data security or personal information; and commitment for each party to introduce or maintain its own domestic laws on privacy protection that meets certain minimum standards.

Like any negotiation in the WTO, getting WTO members to agree on data regulation would not be easy. To garner support among the membership, it would be useful to conduct a stock-taking exercise of existing issues regarding data flow and localization requirements, followed by discussion and identification of best practices, so that the members can better understand the potential of data trade. Most importantly, data regulation should be negotiated as part of a broader deal on digital trade, because trade, rather than the underlying data, is the *raison d'être* of this institution called the WTO.

Endnotes

This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

[1] 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.

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

[3] 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 November 7, 2016, Art. 1.

[4] WTO, Declaration on Global Electronic Commerce, adopted on 20 May 1998 at the Second WTO Ministerial Conference in Geneva, WT/MIN(98)/DEC/2, 25 May 1998.

[5] WTO, Work Programme on Electronic Commerce: Ministerial Decision of 13 December 2017, Ministerial Conference, Eleventh Session, Buenos Aires, 10–13 December 2017, WT/MIN(17)/65, WT/L/1032, 18 December 2017.

[6] WTO, Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019.

[7] For an analysis of the US approach, see Gao (2018c).

[8] Horizontal provisions on cross-border data flows and personal data protection, 18 May 2018, available at: https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=52384.

[9] For an overview of the evolution of digital trade related provisions in China's FTAs, see Gao (2018b).

[10] Wikipedia, List of Largest Internet Companies, available at: https://en.wikipedia.org/wiki/List_of_largest_Internet_companies (accessed 20 February 2020).

[11] For an overview of Chinese data regulation, see Gao (2020, forthcoming).

[12] The submissions can be found on the WTO website starting with INF/ECOM document symbol.

References

Aaronson, S. A. (2019), "What are we talking about when we talk about digital protectionism?", *World Trade Review* 18: 541-577.

Aaronson, S. A. and Leblond, P. (2018), "Another digital divide: The rise of data realms and its implications for the WTO", *Journal of International Economic Law*, 21(2): 245 272. https://doi.org/10.1093/jiel/jgy019

Gao, H. (2011), "Google's China problem: A case study on trade, technology and human rights under the GATS", *Asian Journal of WTO & International Health Law and Policy* (AJWH) 6: 347-385.

Gao, H. (2018a), "Digital or trade? The contrasting approaches of China and US to digital trade", *Journal of International Economic Law* 21(2): 297-321. https://doi.org/10.1093/jiel/jgy015

Gao, H. (2018b), "E-commerce in ChAFTA: New wine in old wineskins?, in Piker, C., Wang, H. and Zhou, W. (eds.), *The China-Australia Free Trade Agreement: A 21st-Century Model*, Hart, 283-303.

Gao, H. (2018c), "Regulation of digital trade in US free trade agreements: From trade regulation to digital regulation", *Legal Issues of Economic Integration* 45(1): 47-70.

Gao, H. (2020), "Data regulation with Chinese characteristics", in Burri, M. (ed.), *Big Data and Global Trade Law*, Cambridge University Press (forthcoming).

Lanz, R. and Maurer, A. (2015), "Services and Global Value Chains: Some Evidence on Servicification of Manufacturing and Services Networks", WTO Working Paper ERSD-2015-03, 2 March 2015. https://www.wto.org/english/res_e/reser_e/ersd201503_e.pdf

Manyika, J., Lund, S., Bughin, J, Woetzel, J, et al. (2016), *Digital Globalization: The New Era of Global Flows*, McKinsey Global Institute, March 2016. https://www.

mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx

Organisation for Economic Co-operation and Development (OECD) (2017), *Key Issues for Digital Transformation in the G20*, Paris: OECD, Report prepared for a joint G20 German Presidency / OECD conference in Berlin, Germany, 12 January 2017.

World Trade Organization (WTO) (2018), *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce*, Geneva: WTO.

Wu, M. (2017), *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, RTA Exchange, Geneva: ICTSD and the IDB.