2-2024

Data sovereignty and trade agreements: Three digital kingdoms

Henry S. GAO
Singapore Management University, henrygao@smu.edu.sg

Data Sovereignty and Trade Agreements: Three Digital Kingdoms

Henry GAO*

Abstract:

For centuries, international lawyers have wrestled with the relationship between national sovereignty and international law. This is also the case of international trade law, where the tension between trade liberalization and national sovereignty culminated in the famous "Great 1994 Sovereignty Debate" between the late Prof. John Jackson and other leading scholars when the WTO came into being.

As we enter the digital age, the issue of sovereignty resurfaced once again in the form of data sovereignty. In this paper, I will examine provisions in trade agreements which deal with data sovereignty issues, such as restrictions on data flow such as internet filtering and censorship; data localization requirements including the requirements to use certain technologies. In particular, the paper will focus on the clash between the US, China, and the EU, which chooses to champion the sovereignty of the firm, the state and the individual respectively. With a critical examination of their relevant policies and positions, the paper will also suggest ways the issue should be dealt with in future trade agreements.

Sovereignty is, paradoxically, one of the most important as well as most misunderstood terms in international law. This is especially true in the areas of international law like international trade law, where sovereignty and international obligations are often pitted against each other when countries try to enforce binding legal obligations through compulsory dispute settlement systems. This led to the Great 1994 Sovereignty Debate in 1994,[1] when the WTO was coming into being. Some twenty years later, it became a hot issue again when the US administration led by President Trump tried to cite sovereignty as the justification for many of its WTO-inconsistent measures, especially those ostensibly grounded on "national security". Due to space constraints, this paper will not be able to unpack the many challenges posed to international trade law by sovereignty. Instead, it will focus on an emerging area: data regulation in trade agreements, which best illustrates the conflict between international trade regulation and sovereignty in the digital era.

The paper will start with an in-depth analysis of the elusive concept of data sovereignty, by trying to blend the classical definitions of canonical authors with the unique features of the data economy. It will then conduct an empirical examination on the current approaches to data sovereignty in trade agreements by the three leading players, i.e., the US, China and the EU. While noting the divergent approaches taken by the three, the paper also concludes with observations on possible future convergence of the three approaches.

I. Data Sovereignty

Sovereignty is one of the most fundamental concepts in modern international law. At the

* Associate Professor, Singapore Management University. This research/project 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] John H. Jackson, The Great 1994 Sovereignty Debate: United States Acceptance and Implementation of the Uruguay Round Results, 36 COLUM. J. TRANSNAT'L L. 157, 182 (1997).

same time, however, it is also one of the most "controversial"[2] concepts with a "long and troubled history".[3] Despite their disagreements on the exact meaning of the term, most international lawyers seem to agree that sovereignty has a "well established" status as either a "highly ambiguous"[4] or "notoriously amorphous" concept.[5] Indeed, the concept is so contested that even many leading international lawyers deem it better to just give up the term, which, called the "S word"[6] by Louis Henkin, is "a mistake, an illegitimate offspring"[7] that is "largely unnecessary and better avoided".[8]

Nonetheless, I am still of the view that we should try to fathom the meaning of sovereignty, as it is "one of those powerful words which has its own existence as an active force within social consciousness" that can not only "represent reality", but also "play a leading part in creating and transforming reality".[9] This is most evident in the repeated reference to sovereignty by national governments in various settings even in the digital age. Thus, without pinning down its meaning, it would not be possible to understand some of the key contentions and approaches in data governance and trade regulation.

In this regard, I will start with classical authors. While the concept of sovereignty has long been used in Europe, Jean Boden is commonly accepted as the "father" of the modern usage of the concept "sovereignty"[10] as he engaged in "the first systematic discussion of the nature" of the concept.[11] In his book "Les six Livres de la Republique", Bodin defines sovereignty as "the absolute & perpetual power in a Republic".[12] This definition focuses on the internal paradigm of the domestic pyramid of power by placing sovereignty as "the most supreme power in the hierarchical organisational structure of society, that is, the highest unified power – as opposed to subordinate decentralised one – free from any temporal authority".[13]

While this definition does provide a good explanation of sovereignty in the domestic context, it might run into difficulty at the international level, where all states are regarded as equal sovereigns in principle, yet in reality countries do differ in their relative powers depending on their military or economic might. The solution to this problem was provided by Vattel, who transposed the concept of sovereignty from the national level onto the international plane.[14] In contrast to the internal paradigm of Rodin, Vattel shifted to the external dimension by defining sovereignty as the "exclusivity of power without", i.e., "a political body which is

---

[2] See, Lassa Oppenheim once noted that, "there exists perhaps no conception the meaning of which is more controversial than that of sovereignty." L.F.E. Oppenheim, International Law – A Treatise, vol. 1, Peace (London: Longmans, Green, 1905), at 103.
[3] J. Crawford, The Creation of States in International Law (Oxford: Clarendon Press, 1979), at 26.
[4] Hent Kalmo and Quentin Skinner, Introduction : a concept in fragments, at 4
[5] Andrew Keane Woods, Litigating Data Sovereignty, 128 Yale L.J. (2018). Available at: https://digitalcommons.law.yale.edu/ylj/vol128/iss2/2, at 360.
[6] Louis Henkin, That "S" Word: Sovereignty, and Globalization, and Human Rights, Et Cetera, 68 Fordham L. Rev. 1 (1999). Available at: https://ir.lawnet.fordham.edu/flr/vol68/iss1/1.
[7] Id., at 2.
[8] Louis Henkin, International Law: Politics and Values 9-10 (1995).
[9] Stéphane Beaulac, The power of language in the making of international law : the word sovereignty in Bodin and Vattel and the myth of Westphalia (Martinus Nijhoff Publishers, 2004), at 1.
[10] See discussion of Beaulac in 101, citing J. Maritain, "The Concept of Sovereignty," in W.J. Stankiewicz (ed.), In Defense of Sovereignty (New York & London: Oxford University Press, 1969), 41, at 43.
[11] C.E. Merriam, History of the Theory of Sovereignty since Rousseau (New York: Columbia University Press, 1900), at 13; Six Books, at 84.
[12] "La SOUVERAINETÉ est la puissance absolue & perpétuelle d'une République.", Six Livres, at 122.
[13] Beaulac at 122, citing D. Carreau, Droit international, 7th ed. (Paris: Pedone, 2001), at 15
[14] Beaulac at 137, citing E. Jouannet, supra, note 602, at 404.

the sole representative of the people externally and which is not submitted to any foreign state or to any higher law externally".[15] By focusing on such "incorporated independent authority", Vattel provided the foundation for the discourse on sovereignty under international law, which is based on the fundamental notion of states as independent actors.

It is easy to see where Bodin and Vattel differ, in that the former defines sovereignty vis-à-vis its subjects while the latter places sovereignty in the context of external powers, be they foreign states or international law. Despite their differences, however, both of these definitions focus on the "general norm"[16] or the "routine" situations[17]. In reality, however, the power of sovereignty is often manifested in decisions concerning "borderline cases", or the "exceptions".[18] This led Schmitt to propose a new definition for sovereignty by stating, at the very beginning of his "Four Chapters on the Concept of Sovereignty", that "Sovereign is he who decides on the exception".[19] As illustrated in later discussions in this paper, the focus on exceptions is also fitting to discussions on data sovereignty, which often needs to wrestle with issues such as exceptions to the general rules on data flow and location of data.

The discussions above reveals a common theme among the definitions by classical authors: power. This is explicit in Bodin ("highest power") and Vattel ("underived power"), and implicit in Schmitt ("exceptional power").[20] Now fast forward to the digital age, where the digital giants pose serious competition to the national governments in terms of the powers they possess. In this sense, the digital firms could be said to have powers rivalling that of traditional sovereigns. This led Lawrence Lessig to extend the concept of Sovereignty by equating it with "control".[21] Lessig developed two models depending on who has the control. The first is the "citizen-sovereignties" model like universities, social clubs, or churches, which "give consumers control over the rules that will govern them".[22] On the other hand there are also the "merchant-sovereignties" where the rules are imposed by the merchants and not chosen by the consumers.[23] These rules are imposed on a "take it or leave it" basis and the only choice consumers can make is whether to go to McDonalds or Burger King. But unlike the switching of your lunch spots in the physical space which is virtually costless, it can be rather costly to try to switch communities in the cyberspace, as "you must give up everything in a move from one cyber-community to another", warned Lessig.[24]

Despite the lack of a precise and commonly-agreed definition, sovereignty is still commonly regarded as one of the most indispensable concepts in international law. The same, however, cannot be said of the concept of data sovereignty. To start with, the concept has been dismissed by many as just an oxymoron, as data by its nature transcends borders, while sovereignty traditionally has been understood to be confined to within borders. Further complications would arise when the data is generated, processed, stored and disseminated in different jurisdictions, as it has become commonplace in the cyberspace these days. Thus, it has been rather difficult to provide a satisfactory definition on data sovereignty, with earlier

[15] Beaulac at 137.
[16] Schmitt, C. (2008). *Political theology: four chapters on the concept of sovereignty*. Univ. of Chicago Press, at 6
[17] Schmitt, at 5
[18] Schmitt, at 5
[19] Id.
[20] Schmitt, at 11.
[21] Lawrence Lessig, Code version 2.0 (New York: Basic Books, 2006), at 283.
[22] Id., at 287.
[23] Id., at 286-7
[24] Id., at 290

attempts focusing either on the ethical dimension of the ownership and control of the data by the individual[25] or the technical dimension of "the coupling of stored data authenticity and geographical location in the cloud"[26]. In their comprehensive survey on the usage of the concept in academic literature, Patrik Hummel et al reviewed 602 papers discussing sovereignty in the digital context, and classified six different types of ways to address data sovereignty.[27] At the end of the day, however, the paper concluded that "data sovereignty" is typically employed to refer "in some way to meaningful control, ownership, and other claims to data or data infrastructures".[28] Such emphasis on control and power is consistent with the classical concepts of sovereignty discussed earlier.

As illustrated by the foregoing discussion, defining data sovereignty has been an endeavour fraught with difficulties. However, as the focus of this paper is on data sovereignty in the context of trade agreements, it is not really necessary to try to come up with a general definition of data sovereignty. To paraphrase the famous remark made by Bill Clinton when he tried to persuade the US congress to grant Permanent Normal Trade Status to the China ahead of China's accession to the WTO in 2000, defining data sovereignty in general would be like "trying to nail jello to the wall".[29] Here, however, we merely need to decide what happens when jello hits the wall, i.e., the applicable rules when the concept of data sovereignty somehow interacts with the rules under trade agreements.

By narrowing the scope of our inquiry, we can tentatively define data sovereignty in the context of trade agreements as follows: The highest independent power over data trade, that can define rules and exceptions, especially regarding first, border measures such as the cross-border transfer of data; and second, domestic regulations such as data localisation requirements. This definition takes into account the key elements of the different variants mentioned earlier, i.e., power, independence and exception. It also situates the concept in the unique context of data trade, with the cross-border fungibility of data as a key feature.

II. Data Sovereignty and Trade Agreements

When it comes to data governance, there are three main groups of players: the individual, which 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 use 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.

---

[25] Towards a Privacy-enhanced Social Networking Site, any 50, which discusses the "data sovereignty principle", I.e., "the data related to an individual belongs to him and that he should stay in control of how these data are used and for which purpose". https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/8581/Ho_Ai_2012_these.pdf;jsessionid=8C6B63BC38E30AC76436C22468476E60?sequence=4>

[26] See Peterson, A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud, at 1, which uses data sovereignty to describe the notion of "establishing data location at a granularity sufficient for placing it within the borders of a particular nation-state", https://www.usenix.org/legacy/events/hotcloud11/tech/final_files/Peterson.pdf.

[27] Hummel, P., M. Braun, M. Tretter, and P. Dabrock, "Data sovereignty: A review" (2021) 8 *Big Data & Society* 205395172098201.

[28] 12.

[29] "Full Text of Clinton's Speech on China Trade Bill," 2021, https://www.iatp.org/sites/default/files/Full_Text_of_Clintons_Speech_on_China_Trade_Bi.htm, accessed June 15, 2021

The clashes between the three groups often result in various restrictive measures, with the most common type being restrictions on cross-border data flow in the name of the protection of individual privacy or national security.[30] More recently, however, data localization requirements have also become popular, with the following as main variations:[31]

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 such restrictions uniformly affect both domestic and foreign firms alike, they are more akin to a most-favoured nation (MFN) treatment type of restriction. While such constraints make it more difficult for firms to move data around, they 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 can be viewed more as 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 offshore servers.[32] Given the different ways MFN and national treatment obligations under trade agreements are structured, a proper understanding of the differences between the two restrictions can help inform regulatory

[30] Wu, M. (2017), Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System, ICTSD, available at: http://e15initiative.org/publications/digital-trade-related-provisions-in-regional-trade-agreements-existing-models-and-lessons-for-the-multilateral-trade-system/, pp. 22-23.

[31] 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, available at: https://doi.org/10.1093/jiel/jgy015, pp. 303-304.

[32] See Chander, Data Nationalism, at 719-721.

approaches and negotiations in trade agreements.

At the same time, notwithstanding their differences, it is also important to keep in mind that both types of restrictions could have major implications for international trade, especially given the growing importance of data to trade in general. Moreover, due to its binding natures, trade agreements have also become the forum of choice for regulating data issues at the international level.

While all countries would agree to 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".[33] 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 States … to preserve … free market …unfettered by Federal or State regulation".[34] In contrast, national security concerns are often cited to justify restrictions on cross-border data flow, 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".[35]

These differences in the domestic regulatory frameworks of these countries are also reflected in their trade agreements, which in turn reveals their different approaches to data sovereignty. Using the twin provisions of free flow of data and prohibition of data localization requirements as proxies, we can group the major approaches to data sovereignty and trade agreements into the following three models, with each represented by a major trader.

	Free flow of data	**Prohibition on data localization**	**Data Sovereignty Regime**
US	Yes	Yes	Firm Sovereignty
China	No	No	State Sovereignty
EU	Yes, but	Yes, but	Individual Sovereignty

III. US: The Firm Sovereignty Model

As the world's largest economy and until recently, the largest trader, the US is a highly

[33] 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.
[34] 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 2021).
[35] 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.

competitive exporter in both agricultural and industrial goods and services. Thus, the US has been very aggressive in promoting free trade and dismantling trade barriers in its trade agreements. This approach is also carried over into the digital age, with the US trade agreements pioneering the inclusion of digital trade issues with an expansive set of obligations.

1. Firm Sovereignty

In particular, two provisions have become the *sine qua non* in the digital trade chapters in US trade agreements, with the recently-concluded United States-Mexico-Canada Agreement ("USMCA") as the leading example:

First 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";[36] and

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".[37]

These two provisions provide strong protection of the interests of the firm, which deem the restrictions on cross border flow of data and various localization requirements as obstacles to their ability to conduct businesses across national boundaries. Applying the concept of sovereignty mentioned earlier, the US approach essentially put the sovereignty into the hands of business firms, so that they have the control on both border measures and domestic regulations.

As we can see from the experiences of China and the EU below, 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 different approaches in its trade agreements.

2. Privacy as a consumer right

On privacy protection, the US trade agreements only require parties to adopt their own legal framework for data protection, which could take many different legal 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."[38] This is very different from the EU approach which requires its trade partners to adopt GDPR-equivalent clauses. While the US agreements also calls for Parties to "take into account principles and guidelines of relevant international bodies",[39] the examples only include "the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)", which are regarded as providing only minimum levels of data protection or "1st generation" data privacy standards.[40] Moreover, rather than enhancing privacy protection for consumers, the US trade agreements seem to be more concerned with making

[36] USMCA, Art. 19.11.
[37] USMCA, Art. 19.12.
[38] USMCA, footnote 4.
[39] USMCA, Art. 19.8.2.
[40] Graham Greenleaf, 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 Privacy8 April 2018, at 1. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf.

sure that the commercial interests of the firms are not adversely affected by over-restrictive privacy regimes. Take for example the clause on personal information protection under the USMCA, which include a total of six paragraphs. Only one of these contains substantive obligations to adopt or maintain legal framework on personal information protection,[41] while three are aimed at minimizing the regulatory burden for business firms. 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",[42] which are apparently modelled after the necessity test and proportionality principle under the WTO. The second requires the Parties to "endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction", which also draws from the non-discrimination principle of the WTO, especially the national treatment obligation. Lastly, while the agreement recognizes the divergent legal approaches the Parties might take on personal information protection, it also encourages the Parties to develop "mechanisms to promote compatibility between these different regimes". Again, trade lawyers would recognize in these provisions vestiges of WTO rules on mutual recognition, harmonisation and equivalence under the various WTO agreements.

3. Security as a business risk

On security, the US trade agreements focus on "threats to cybersecurity undermine confidence in digital trade", i.e., "malicious intrusions or dissemination of malicious code that affect electronic networks".[43] Put differently, the US approach mainly addresses cybersecurity risks facing the private firm, which is quite different from the Chinese approach which focus on perceived threats to national security. At the same time, the US approach also tries to minimize the 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".[44] The risk-based approach is apparently carried over from the regulatory framework under the WTO, especially under the TBT and SPS agreements. By placing restrictions on the regulatory measures that might be adopted by governments, such an approach provide better protection for the firms' interests. Similarly, the reference to "consensus-based standards" also reflects prevailing practices in the US, which has been codified in the the Cybersecurity Enhancement Act of 2014.[45] 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."[46] Under the Act, the US cybersecurity standards is developed as a public-private partnership between the government and the business sector, which serves to reduce the cybersecurity risks for the firms rather than advancing the national security goals of the government.

4. Trade agreements

Many other provisions in the USMCA are also designed to facilitate the development of

[41] USMCA, Art. 19.8.2.
[42] USMCA, Art. 19.8.3.
[43] 19.15.
[44] Id.
[45] "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 June 15, 2021.
[46] Sec. 101. Public-Private Collaboration on Cybersecurity.

digital trade. This is done by either removing regulatory barriers, such as the provision on non-discriminatory treatment of digital products; or providing an enabling framework for digital trade such as the provisions on 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.[47] This clause is mainly designed to deal with the risks that 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. This provision apparently grew out of the net neutrality principle from the domestic telecom regulatory framework within the US. In a way, it provides the digital giants reverse control over the telecom and internet services providers in the countries they are operating, so that they would not be held hostage by the network throttling practices often found in many countries.

As the main proponent of the pluri-lateral Trade in Services Agreement (TISA) negotiations, the US also proposed similar provisions in the draft TISA agreement. Most of these can be found in the e-commerce chapter, where the US called for provisions which guarantee service suppliers the freedom to transfer information across countries for the conduct of its 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 localisation 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 localisation 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.

IV. China: The State Sovereignty Model

1. Data Sovereignty

For China, the key to data regulation is data security, which has now been elevated to the level of national security and national sovereignty. Such a regulatory approach, which I dubbed "data regulation with Chinese characteristics" in another paper,[48] is the result of an evolution spanning 25 years. The evolving approach closely traces the development of the Internet sector in China. When the Internet first started as a novelty that was confined to the ranks of tech-savvy geeks, the regulations focused on computer and internet hardware, by requiring all Internet connections to go through official gateways sanctioned by the Chinese government. As the Internet gradually expanded to the masses with the proliferation of software and apps catered to popular uses, the government moved on to regulate the software and started to demand that software used for Internet access must be sanctioned by the government. As the cyberspace became an indispensable part of everyday life and began to permeate every sector from socializing, shopping to entertainment and education, the government shifted the focus to

[47] USMCA, Art. 19.10.

[48] Gao, Henry S., Data Regulation with Chinese Characteristics (August 1, 2019). SMU Centre for AI & Data Governance Research Paper No. 2019/04, Singapore Management University School of Law Research Paper No. 28/2019, in Mira Burri (ed), Big Data and Global Trade Law, Cambridge University Press, 2020. , Available at SSRN: https://ssrn.com/abstract=3430284 or http://dx.doi.org/10.2139/ssrn.3430284.

the regulation of content and now data, which is the essence of cyberspace that powers everything, 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 Cybersecurity Law in 2016. The agency that is responsible for content regulation, the CAC, has also evolved into the super-agency that is almost synonymous with data regulation in China. The CAC has no responsibility in promoting the growth of the sector. Instead, its only responsibility is making sure that the cyberspace is secure and nothing unexpected would pop up. It is this single-minded pursuit of security that has led to such draconian policies as Internet blockage, filtering and other restrictions on the free flow of data, forced data localization requirements and the transfer of source code. As the Internet is becoming more complicated and omnipotent, we can only expect Internet and data regulations in China to become more sophisticated and omnipresent.

2. Trade Agreements

At the international level, 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. This only changed with its FTAs with Korea and Australia, which were both signed in 2015. Nonetheless, the provisions in these two FTAs remain rather modest, as they mainly address trade facilitation related issues, such as 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 level of protection equivalent to traditional forms of commerce.

A major breakthrough was made in the Regional Comprehensive Economic Partnership (RCEP) Agreement, which China signed along with other 14 countries in the region in November 2020. Under the Chapter on E-commerce, China like 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",[49] or "prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person".[50]

Of course, merely agreeing to the twin provisions on data flow and data localization does not mean that China now embraces the US model. Instead, both provisions are still overshadowed by national security concerns. First of all, both provisions allow Members to adopt "any measure that it considers necessary for the protection of its essential security interests". Moreover, they also explicitly state that such security measures 'shall not be disputed by other Parties", which means that the securities measures will be largely self-judging. Finally, as the whole chapter on e-commerce is carved out from the normal dispute settlement procedure under the RCEP, any such security measure will not be subject to legal challenge.

Another exception to these two obligations is "any measure … that [the implementing Party] considers necessary to achieve a legitimate public policy objective". Note here the necessity test is not the objective one as found under the general exceptions clause under GATT Art. XX, but what the Party taking such measure "considers necessary", which is only found under the

[49] RCEP, Art. 12.14.
[50] Ibid, Art. 12.15.

security exceptions clause under GATT Art. XXI. The subjective nature of the necessity test here is further confirmed by the footnotes to the two provisions, which explicitly "affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party".

3. Personal Information Protection

What then, could such "legitimate public policy objective" entail? Like most other countries in the world, this could include laws for the protection of privacy or personal information. Yet, the Chinese approach to privacy protection also comes with its own limitations. To start, privacy is a rather new concept in Chinese law, and there was no privacy protection law until 2009, when privacy was first recognized as a civil right under the Tort Liability Law. This was duly incorporated into China's new Civil Code enacted in 2020, which has a separate chapter on privacy and personal information protection as part of the volume on personality rights.[51] According to Art. 1035 of the new 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". In China, there are many laws with do not require the consent of the data subject. For example, under Art. 25 of China's Electronic Commerce Law, government agencies may require e-commerce operators to provide e-commerce transaction data, which includes the personal information of the consumers. Similarly, by requiring government agencies in charge of cyber security monitoring and management and their staff to keep confidential any personal or privacy information they obtain in the discharge of their duty, Art. 45 of the Cyber Security Law also indirectly confirms that such agencies do have access to personal information of netizens without their consent. This approach is also adopted by China's draft Personal Information Protection Law, which confirms that data processors do not need to obtain the consent of the data subject when necessary for discharging official duty and responsibility.[52] Moreover, in cases specified by the relevant laws or administrative regulations, the data subject would not even be made aware that his/her data is being processed.[53] The same exception also applies in cases where the notification or obtaining the consent of the data subject would impede the discharge of official duty by the relevant state organs.[54] Even if the data subject later becomes aware of the occurrence of such data processing activities, he/she would be denied the right to review or copy such personal information, which is normally available to data subjects.[55]

To sum up, the Chinese framework for personal information protection provide extensive exemptions for the government to collect personal information, either directly or through personal information processors. This probably explains why China until this day has yet to participate in the APEC CBRP,[56] as the CBPR Program Requirements includes some potentially awkward questions such as "how the collected personal information may be shared, used or disclosed as compelled by law", which neither the companies nor the Chinese government might be ready to answer.

4. "Important Data" and "Core Data"

[51] Chapter 6 of Volume 4 of the civil code.
[52] Art. 13.3.
[53] Art. 19.
[54] Art. 35.
[55] Art. 45.
[56] https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

Despite the gaps in China's personal information protection framework, at least an argument could be made that it is common to have personal information protections laws as exceptions to the twin provisions on data flow and data localization. However, the exceptions unber the Chinese data regulation regime covers not only personal date but also "important data", a highly important concept that is poorly defined.

The concept of "important data" was first introduced in the Cyber Security Law, which requires "operators of critical information infrastructure" to locally store not only personal information but also "important data" collected and generated in their operations within China.[57] If they need to send such data abroad due to business necessity, they have to first undergo security assessment by the authorities.[58] Thus, the local storage requirement and restriction on cross-border data flow applies to "important data" collected and generated by operators of "critical information infrastructure", which is defined in Article 31 of the law as infrastructure in 'important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs', as well as such 'that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage'. Such a broad definition could potentially capture everything and is not really helpful nor does it give much guidance, which is why the same Article also directs the State Council to develop the 'specific scope of critical information infrastructure'.

In 2016, the CAC issued the National Network Security Inspection Operation Manual[59] and the Guide on the Determination of Critical Information Infrastructure,[60] which clarified the scope of critical information infrastructure by grouping them into three categories: (1) websites, which includes websites of government and party organizations, enterprises and public institutions, and news media; (2) platforms, which include Internet service platforms for instant messaging, online shopping, online payment, search engines, emails, online forum, maps, and audio video; and (3) production operations, which include office and business systems, industrial control systems, big data centres, cloud-computing and TV broadcasting systems.

The CAC also laid down three steps in determining the critical information infrastructure, which starts with the identification of the critical operation, then continues with the determination of the information system or industrial control system supporting such critical operation, and concludes with the final determination based on the level of the critical operations' reliance on such systems and possible damages resulting from security breaches in these systems. More specifically, they listed eleven sectors, which include energy, finance, transportation, hydraulic, medical, environmental protection, industrial manufacturing, utilities, telecom and Internet, radio and TV, and government agencies. The detailed criteria are both quantitative and qualitative. For example, on the one hand, critical information infrastructure includes websites with daily visitor counts of more than one million people and platforms with

[57] Article 37.
[58] Id.
[59] Central Leading Group on Cyber Security and Informatisation General Office, Network Security Coordination Bureau, National Network Security Inspection Operation Manual [Guojia Wangluo Anquan Jiancha Caozuo Zhinan], June 2016.
[60] Guide on the Determination of Critical Information Infrastructure (Trial) [Guanjian Xinxi Jichu Sheshi Queding Zhinan (Shixing)], in Notice on Conducting Network Security Inspections of Key Information Infrastructure [Guanyu Kaizhan Guanjian Xinxi Jichu Sheshi Wangluo Anquan Jiancha de Tongzhi], *Zhongwangban Fawen* No 3 (2006), Annex 1, July 2016.

more than ten million registered users or more than one million daily active users, or daily transaction value of ten million RMB. On the other hand, even those that do not meet the quantitative criterion could be deemed to be critical information infrastructure, if there are risks of security breaches that would lead to leakage of lots of sensitive information about firms or enterprises, or leakage of fundamental national data on geology, population and resources, or seriously harming the image of the government or social order, or national security. The potentially wide reach of the criteria was well illustrated by the case of the BGI Group, which was fined by the Ministry of Science and Technology in October 2018 for exporting certain human genome information abroad via the Internet without authorization.[61] Given the nature of their business, the BGI case could fall under the category of 'leakage of fundamental national data on … population', as mentioned earlier.

In addition to the vague concept of "important data", the newly-enacted Data Security Law adds another concept of "national core data", which 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. Moreover, as mentioned above, the restrictive rules on data flow and data localisation only applies to "important data" collected and generated by operators of "critical information infrastructure" as per the Cyber Security Law. It is unclear, however, whether the stricter restrictions on "national core data" will be similarly limited to by operators of "critical information infrastructure". A plausible or even compelling argument could be made to argue that due to its utmost importance, the restrictions on "national core data" would apply to all data processors or even private individuals, even if they do not qualify as by operators of "critical information infrastructure".

V. EU: The Individual Sovereignty Model

1. The GDPR

Unlike the US and China, which focus respectively on the firm and the state, 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 countries unless they have privacy protection standards deemed adequate.[62] The Directive was replaced[63] by the GPDR in 2018.

Despite its name which 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')".[64] It regulates the behaviours of the data controller and processor, which are respectively defined as the one who 'determines the purposes and means of the processing of

[61] An Shujun, 'How to Conduct "Safety Check" for Exporting Data [Shuju Chujing Ruhe 'Anjian']', *zhihu*, available at: https://zhuanlan.zhihu.com/p/65413452.
[62] European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 23 November 1995 P. 0031 – 0050.
[63] See Susan Ariel Aaronson, Patrick Leblond, Another Digital Divide: The Rise of Data Realms and its Implications for the WTO, *Journal of International Economic Law*, Volume 21, Issue 2, June 2018, Pages 245–272, https://doi.org/10.1093/jiel/jgy019, at 260.
[64] Id, Article 4.1.

personal data"[65] and "processes personal data on behalf of the controller".[66] Under the GDPR, the processing of personal data is only allowed with the "explicit"[67] consent of the data subject and a few other specifically enumerated reasons,[68] pursuant to a set of principles which specifies the scope and manner of such processing.[69] Transfer of personal data to third countries is only allowed on the basis of an adequacy decision[70] or appropriate safeguards.[71]

2. Digital sovereignty

Since its introduction, the GDPR has become the gold standard of privacy protection in the world. Encouraged by its success, top EU officials started to advocate "technological sovereignty" for the EU.[72] "Technological sovereignty" is a concept closely linked with "digital sovereignty"[73], which was elaborated in the European Commission's "Communication on a European Strategy for Data" unveiled in February 2020.[74] As many commentators pointed out, the EU's new data strategy is designed to "counter the strong position of US and Chinese digital companies in the European market"[75] and remedy "the key European disadvantage" of "the lack of significant European digital corporations with global influence'.[76] The new data strategy aims to create "a single European data space" so that "by 2030, the EU's 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".[77]

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

---

[65] 4.7
[66] 4.8.
[67] Article 49.1.(a).
[68] Art. 6.1. see also Aaditya Mattoo, Joshua P Meltzer, International Data Flows and Privacy: The Conflict and Its Resolution, *Journal of International Economic Law*, Volume 21, Issue 4, December 2018, Pages 769–789, https://doi.org/10.1093/jiel/jgy044, at 774.
[69] 5.1. see also Mattoo & Meltzer, at 774.
[70] Art. 45.
[71] Art. 46.
[72] Frances Burwell and Kenneth Propp, "The European Union and the search for digital sovereignty: Building 'Fortress Europe' or preparing for a new world? - Atlantic Council," June 2020, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/, accessed June 14, 2021. For the statement by EU President Ursula von der Leyen, see Mark Scott, "What's Driving Europe's New Aggressive Stance on Tech," Politico, October 28, 2019, https://www.politico.com/news/2019/10/28/europe-technology-silicon-valley-059988. For the statement by incoming EU commissioner for the internal market Thierry Breton, see "Questions to the Commissioner-Designate Thierry Breton," European Commission, 2019, https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf.
[73] for the distinction between the two, see Burwell & Propp, at 1.
[74] "Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions," European Commission, February 19, 2020, 9, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
[75] Burwell & Propp, at 2.
[76] Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry – ECFR/336, at 11
[77] Data strategy at 4.

The EU's data strategy can be seen as part of its broader plan of establishing its own "strategic autonomy". The concept started as an idea of the French, when they published their 1994 white paper on defence.[78] Gradually, however, it was accepted by all of the big three EU member states: Germany, France and Italy.[79] The concept was adopted by the EU in 2016 when it unveiled its Global Strategy, which was supposed to "nurtures the ambition of strategic autonomy" for the EU.[80] With Trump's election as US president and Brexit, the concept started to take off among the governments of EU member states.[81] While there was some ambiguity on the exact content of the concept, the bigger EU member states typically perceive it as referring to decision-making autonomy.[82] This is recently confirmed by the new trade strategy paper issued in February 2021, where the EU further refined it as a concept of "open strategic autonomy" which emphasises "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",[83] with a priority area being the EU's digital agenda.[84]

3. Data flow and localization

On data flow, the EU takes a bifurcated approach. Non-personal data are supposed to flow freely pursuant to the EU's Framework for the Free Flow of Non-personal Data,[85] while the cross-border flow of personal data is subject to the stringent requirements under the GDPR, despite the explicit recognition under the GDPR that "[f]lows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation."[86] Due to its high compliance costs,[87] the GDPR has proven to be "challenging especially for the small and medium sized enterprises (SMEs)".[88] To stay away from potential legal challenges, many US websites blocked access by EU customers before the GDPR went into effect,[89] and remained unavailable in the EU months after.[90]

---

[78] "Livre Blanc Sur La défense Et La sécurité Nationale" <http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le-livre-blanc-sur-la-defense-1994.pdf> accessed April 23, 2021.
[79] "Independence Play: Europe's Pursuit of Strategic Autonomy ..." <https://ecfr.eu/special/independence_play_europes_pursuit_of_strategic_autonomy/> accessed April 23, 2021, at 6.
[80] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy, https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
[81] Independence play: Europe's pursuit of strategic autonomy, at 7.
[82] 10-11.
[83] Trade Policy Review - An Open, Sustainable and Assertive Trade Policy, at 4. https://trade.ec.europa.eu/doclib/html/159438.htm.
[84] Id., at 16.
[85] 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.
[86] Recital 101.
[87] Irwin, L., "How much does GDPR compliance cost in 2021? - IT Governance Blog En" June 2021, https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020, accessed June 14, 2021.
[88] 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, 24.6.2020 COM(2020) 264 final, at 9,
[89] Schechner, S. and N. Drozdiak, "U.S. Websites Go Dark in Europe as GDPR Data Rules Kick In" May 2018, https://www.wsj.com/articles/u-s-websites-go-dark-in-europe-as-gdpr-data-rules-kick-in-1527242038, accessed June 14, 2021.
[90] "More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect," 2018, https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/, accessed June 14, 2021.

In addition to its negative impact on cross-border data flow, the GDPR also creates the 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).[91] However, as Chander has eloquently argued, data localization not only will not "solve the policy objectives identified in Schrems II', but also creates "its own policy problems".[92] The data localization requirements for non-personal data are banned by the EU's Framework for the Free Flow of Non-personal Data, which mandates 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,[93] with most cover special categories of sensitive data like health-related personal data or financial services data.[94] On the latter point, it is worth noting that the EU approach again diverges from the current US approach. When the US negotiated the TPP, it carved out the entire financial services sector from the scope of its e-commerce chapter, including prohibition of data localization requirements.[95] In the new USMCA, however, the USA 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".[96] It would be interesting to see whether the EU shifts closer to the US approach in the future.

4. Trade agreements

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-Trade, which favours free trade for the sector, and DG-Justice, which has concerns over personal information protection.[97] 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.[98] In February 2018, however, the two DGs were finally able to reach a compromise position, which includes on the one hand horizontal clauses on free flow of all data and ban on localization requirements, while one the other hand, affirms the EU's right to regulate in the sector by making clear that it shall not be subject to investor-state arbitration.[99] Despite this development, the EU still seems to prefer handling data flow issues through bilateral "adequacy" recognitions, which so far has only been granted to a dozen countries.[100] In many of its latest FTAs, data

[91] Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).
[92] Anupam Chander, Is Data Localization a Solution for *Schrems II*?, *Journal of International Economic Law*, Volume 23, Issue 3, September 2020, Pages 771–784, https://doi.org/10.1093/jiel/jgaa024, at 778-784.
[93] Bruwell, at 9.
[94] Nigel Cory, Cross-Border Data Flows: Where are the Barriers, and What Do They Cost, Information Technology & Innovation Foundation, May 2017, Appendix A, http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.63382255.1306428313.1587045825-1501175350.1587045825.
[95] TPP, Art. 14.1.
[96] USMCA, Art. 17.18.2.
[97] Aaronson at 261.
[98] Id.
[99] Id., at 262.
[100] So far, the EU has granted adequacy recognitions to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. See

flow issues were left out in the main text, with a separate adequacy decision adopted. This is, for example, the case of its Economic Partnership Agreement (EPA) with Japan, where the adequacy decision [101] was adopted separately from the EPA, which does not include commitments on free flow of data.[102] While its recent FTA with Vietnam lacks not only provisions on data flow & localization, but also any plan for an adequacy decision.

V. 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 China and the United States. Among the ten biggest digital trade firms in the world, six are American and four are Chinese.[103] 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 the "digital" side while China focuses on the traditional "trade" side when it comes to digital trade, as I argued in another paper.[104]

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 restrictive privacy rules could be viewed as a form of "digital protectionism"[105] 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",[106] 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 …

---

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[101] "Press corner," 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421, accessed June 14, 2021.

[102] 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."

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

[104] Henry Gao, Digital or Trade? The Contrasting Approaches of China and US to Digital Trade, *Journal of International Economic Law*, Volume 21, Issue 2, June 2018, Pages 297–21, https://doi.org/10.1093/jiel/jgy015.

[105] Aaronson, S. A. (2019), "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review* 18: 541-577.

[106] Anupam Chander, The Electronic Silk Road: How the Web Binds the World Together in Commerce (Yale University Press, 2013), at 57.

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".[107] Therefore, it is no surprise that the United States 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.[108] 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,[109] 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.[110] 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.[111] 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,[112] and recognize privacy as not only a consumer right, but also a fundamental human right that is recognized in several fundamental EU instruments[113] and the constitution of many member states.[114] Such a refreshing perspective is probably the biggest contribution made by the European Union to digital trade issues.

VI. Conclusion

[107] Telecommunication Act of 1996, 47 U.S.C.¶230(b)(2), available at https://www.law.cornell.edu/uscode/text/47/230 (visited 20 April 2018).
[108] Aaronson, Another Digital Divide, at 254.
[109] Chander 2013, at 57-58.
[110] For an overview of Chinese data regulation, see Gao, Henry S., Data Regulation with Chinese Characteristics (August 1, 2019). SMU Centre for AI & Data Governance Research Paper No. 2019/04, Singapore Management University School of Law Research Paper No. 28/2019, in Mira Burri (ed), Big Data and Global Trade Law, Cambridge University Press, 2020. , Available at SSRN: https://ssrn.com/abstract=3430284 or http://dx.doi.org/10.2139/ssrn.3430284.
[111] International Data Flows and Privacy: The Conflict and its Resolution • 771, citing James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004). Faculty Scholarship Series, Paper 649;
[112] See Paul M. Schwartz and Karl-Nikolaus Peifer, 2017. 'Transatlantic Data Privacy Law', The Georgetown Law Journal 106 (115) at 132–37.
[113] See e.g., 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.
[114] These includes Germany, Greece, Hungary, Poland and Spain, see matto and Meltzer, 772.

Trade agreements are complicated. Data sovereignty issues are even more so. This paper provides a modest attempt to offer some clarity to these issues with an in-depth discussion of the data sovereignty models of the three major players. The discussions herein should provide some help in understanding the approaches of most other countries in the world as well because, as illustrated by Ferracane & Marel in their recent comprehensive survey, countries around the world broadly fit in one of the three models discussed here.[115]

At the same time, we should not be disheartened by the wide divergences among the three approaches. Such differences might prove to be short-lived as countries are learning from each other's' experiences. For example, with its recent ban on TikTok & WeChat, the US seems to be taking a leaf from China's playbook. At the same time, by accepting obligations on free flow of data and prohibitions on data localization requirements, China seems to be edging closer to the US position. Just like the three kingdoms in Chinese history which was ultimately united into one, hopefully, the three digital kingdoms studied in this paper can also, through trade agreements, forge their divergent approaches to data sovereignty into one, at least in the cyberspace.

[115] "Ferracane, Martina Francesca; van der Marel, Erik. 2021. Regulating Personal Data : Data Models and Digital Services Trade. Policy Research Working Paper;No. 9596. World Bank, Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/35308 License: CC BY 3.0 IGO."