

Digital Megaregulation Continued: the Regulation of Cross-Border Data Flows in International Economic Law

By Thomas Streinz



Author Thomas Streinz

Introduction

Digitalization is rapidly transforming the global economy due to greatly enhanced ability to transfer information within and between companies, along supply chains, and vis-à-vis consumers. Global platforms for communication and electronic commerce are central nodes that facilitate these economic exchanges, and cloud computing has significantly reconfigured the ways in which businesses and consumers use information and communication technology (ICT). All these developments rely on data flows. The geographical expansion and commercialization of the Internet in the 1990s created a new default for the transfer of digitalized information across the world. Legal scholars have long grappled with the implications for domestic and international law. Data flows are regulated by a complex interplay of physical and digital infrastructures, technical standards, social norms, and various instruments of private and public law. Recently, new treaties under international economic law have emerged as important venues for the creation and contestation of new rules for the digital economy.

This article addresses the arguably most consequential provisions on cross-border data flows in the Trans-Pacific Partnership (TPP), which were incorporated into the Japan-led Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Similar rules also feature in the Japan-US Digital Trade Agreement (JUSDTA) that was concluded in October 2019, the Digital Economy Partnership Agreement (DEPA) that Chile, New Zealand, and Singapore signed in June 2020, and the successor agreement to NAFTA between the United States, Mexico, and Canada (USMCA) that entered into force in July 2020. These new rules on cross-border data flows are often portrayed as an adaptation and continuation of established disciplines under international trade and investment law and are, often interchangeably, heralded as advancing “digital trade” and “electronic commerce”. However, this article suggests that these new rules are better understood as elements of global economic ordering that transcend and transform international trade and investment law as traditionally understood and thereby continue a project of “digital megaregulation”. This terminology and conceptual framework builds on joint work in NYU School of Law’s MegaReg project (*Megaregulation Contested: Global Economic Ordering after TPP*, OUP, 2019, in cooperation with the United Nations University and the National Graduate Institute for Policy Studies (GRIPS) in Tokyo).

TPP as Megaregulation

Understanding the TPP as “megaregulation” draws attention

towards various features of this kind of global economic ordering that are particularly salient in the digital domain. Megaregulatory agreements address a wide range of regulatory issues to increase economic flows, including data flows, between participating countries (and beyond). This is achieved through various procedural and substantive rules designed to enhance regulatory alignment which enables businesses, especially multinational corporations, to operate transnationally with relative ease (for example, by freeing them from territorial data localization requirements). While coordination through treaties between nation states is commonplace in international trade and investment law, it is considered exceptional in the context of global Internet governance. The technologies that enabled the digital transformation of the global economy were not preordained by international agreements. But agreements like the TPP have significant implications for countries’ evolving regulation of their digital economies. To the extent to which regulatory frameworks for the digital economy are not yet in place, in their infancy, or in need of recalibration and revision, they will be crafted in accordance with the procedural and substantive commitments that megaregulation entails.

The TPP created a new template of rules for the digital economy. This model is not just significant for the countries that drafted, signed, and ratified the agreement. Megaregulation creates spillover effects and is meant to shape the global discourse around economic governance. What began in the TPP was preserved in the CPTPP, continued in the JUSDTA, DEPA, and USMCA, and is likely to remain an important template for future discussions around new rules for the global digital economy in the World Trade Organization (WTO) and under the Osaka Track that Prime Minister Shinzo Abe launched at the G20 summit in June 2019.

TPP’s Model for the Digital Economy

The TPP is a complex agreement with 30 chapters of operative legal text alongside numerous annexes and declarations. Chapter 14 is dedicated to “electronic commerce” and its provisions cover a wide range of issues: customs duties for electronic transmissions; non-discriminatory treatment of digital products; domestic frameworks for electronic transactions, authentication, and signatures; digital facilitation of customs administration for trade in physical goods; unsolicited commercial electronic messages (spam) and consumer protection online; regulatory cooperation, especially on cybersecurity; non-disclosure of source codes, and so on. The arguably most consequential provisions concern restrictions on cross-border transfer

of information and requirements to use domestic computing facilities. Such measures are often conceptualized as different forms of “data localization” that defy the default that data flows freely on the Internet and can be stored, processed, or transferred across borders. The TPP constrains states’ ability to restrict cross-border data flows or to require the use of domestic computing facilities by requiring a legitimate public policy objective that must be pursued in a non-arbitrary or not unduly discriminatory manner, is not a disguised restriction on trade, and does not exceed what is necessary to achieve the objective. Such language is inspired by the WTO’s General Agreement on Trade in Services (GATS) but it is unclear how dispute settlement panels are going to interpret and apply the TPP’s new rules if states’ regulation of the digital domain impacts cross-border data flows.

The TPP charted new ground by creating binding rules for “free data flows” and against “data localization” that are not directly tied to trade in goods or services. States that sign and ratify agreements like the TPP subject their regulation of the digital economy to external scrutiny. This is significant, because the digital transformation of the economy is likely to propel demand for public-sector led regulation in the digital domain to address (perceived) market failures (for example, the concentration of data in large tech companies), harms caused by the use of data-driven technologies (for example, adverse impacts on privacy and informational self-determination because of ubiquitous data collection), and distributional concerns (for example, the need to counteract tax avoidance strategies by global digital corporations). When such measures have an impact on the cross-border transfer of information or require the use of domestic computing facilities, they will be subject to additional scrutiny and pressure under the TPP model.

EU Opposition to the TPP Model

The European Union was confronted with the TPP model in its negotiations with the US on a new transatlantic trade and investment agreement (TTIP) and the plurilateral trade in services agreement (TISA), both of which did not come to fruition. The EU’s negotiations with Japan yielded a far-reaching Economic Partnership Agreement (JEEPA) which entered into force in February 2019 but bracketed the question of dedicated rules for cross-border data transfers (to which Japan had already committed under the TPP at this point). In parallel, the EU and Japan recognized their respective data protection regimes as “adequate” to allow for facilitated transfers of personal data between both jurisdictions. This reflects the EU’s preference to negotiate cross-border transfers of personal data under a data protection rather than international economic law framework. The EU’s reluctance to include TPP-style free data flow provisions in its trade, investment, and economic partnership agreements is driven by concerns that its General Data Protection Regulation (GDPR) might be incompatible with the TPP model. Even though data protection and privacy are universally recognized as legitimate public policy objectives that could justify restrictions of cross-border data transfers in principle, the EU’s assessment of the adequacy of other countries’ data protection regimes might still be viewed as arbitrary or unjustifiably discriminatory. Moreover, the principal imposition of dedicated rules

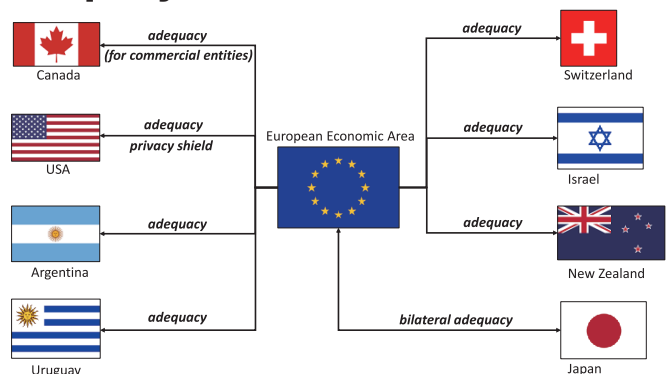
for cross-border transfers of personal data itself might be judged unnecessary by the arbitrators of a trade or investment dispute settlement tribunal.

To guard against these risks, the EU has refrained from TPP-style commitments. In its submissions to the WTO’s efforts to craft new multilateral rules for the digital economy, the EU maintains that no disciplines and commitments shall affect the protection of personal data and privacy. Its proposal for cross-border data flows would only ban the kind of territorial “data localization” that the EU itself does not employ. The GDPR’s restrictions on transfers of personal data from the EU to third countries would not be subject to scrutiny. The GDPR is widely seen as a key example of what Anu Bradford has theorized as the “Brussels Effect”. Countries around the world gravitate towards the GDPR as a model for data protection for a variety of reasons, one of which is the adequacy regime under which the European Commission assesses whether other countries’ data protection standards are equivalent to the EU’s as a pre-condition for cross-border transfers of personal data. This regime differentiates between countries with and without (in the European Commission’s assessment) an adequate level of data protection. The GDPR’s regulatory default is that cross-border transfers of personal information are forbidden; the adequacy assessment is the most coveted exception because others (such as standard contractual clauses) incur significant compliance costs. In contrast, the TPP model foresees uninhibited transfers of information, including personal information, as the default and restrictions of such transfers as the exception, which requires justification and invites scrutiny. This fundamental tension, however, does not mean that countries cannot sign on to both models, as evidenced by Canada and Japan, which both enjoy adequacy under the GDPR while being bound to the TPP model under the CPTPP and their respective agreements with the US (Chart 1).

Survival & Proliferation of the TPP Model

The TPP became a major flashpoint in the US presidential election of November 2016, and the newly elected president withdrew the US from the TPP during his first week in office. Subsequently, Japan took

CHART 1
Selected jurisdictions that enjoy adequacy status under the EU’s GDPR



Source: Compiled by the author based on European Commission information (<https://perma.cc/3PNA-BW3N>)

a leading role in resurrecting the agreement as the CPTPP. All 11 remaining parties signed the CPTPP, which suspended a range of provisions on investment protection and intellectual property but left the electronic commerce chapter and its new rules for free data flows and against data localization entirely intact. The CPTPP is in force for Australia, Canada, Japan, Mexico, New Zealand, Singapore, and Vietnam. Ratification efforts in Chile stalled and Brunei, Malaysia, and Peru also did not follow through with bringing the agreement into force.

Despite its withdrawal from the TPP, the US continued to include its new model of provisions for free data flows and against data localizations in the USMCA with Canada and Mexico and the dedicated digital trade agreement with Japan – countries that are bound by the CPTPP anyway. The main difference between the CPTPP and these more recent agreements as regards cross-border data flows is the elimination of the possibility to justify requirements to use domestic computing facilities, as the USMCA and JUSDTA ban this kind of data localization entirely. The US is also advocating for free data flow provisions in the WTO, where agreement is unlikely due to rising geopolitical tensions, conflicting interests, and lingering frustration with the abandoned Doha development agenda.

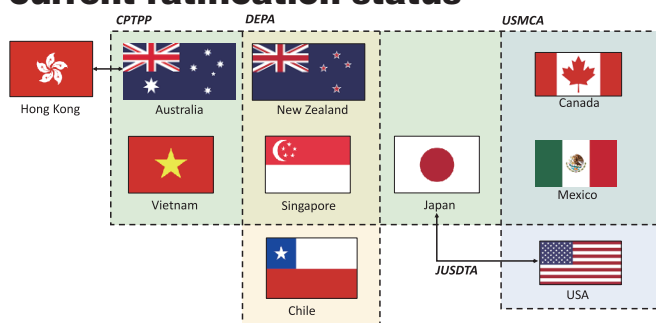
Meanwhile, the TPP model is likely to proliferate through other venues, even where the US government is not actively pushing for it. CPTPP signatories Chile, New Zealand, and Singapore included TPP-style provisions in the DEPA, designed as a template of several modules that countries interested in new rules for the digital economy may choose for their agreements. Similarly, the free trade and economic integration agreement that entered into force between Australia and Hong Kong in January 2020 includes rules that are almost identical to the TPP model. The continued attraction of the TPP model likely reflects countries' conviction that the Silicon Valley Consensus of free data flows and relatively light-touch regulation is still the best approach for digital development (*Chart 2*).

The TPP Model & Corporate Multi-Nationality

According to established principles of international law, countries that sign and ratify agreements bind themselves (only) vis-à-vis each

CHART 2

Countries with binding commitments that follow the TPP model based on current ratification status



Source: Compiled by the author

other. In reality, the commitments towards free data flows and against data localization that the TPP model entails are likely to be invoked by companies reliant on cross-border data transfers and transnational ICT infrastructure. Due to corporate multi-nationality, even companies whose home country has not signed or ratified a TPP-style agreement, or indeed has withdrawn from it, can rely on its provisions to hold governments accountable for their commitments towards free data flows and against data localization.

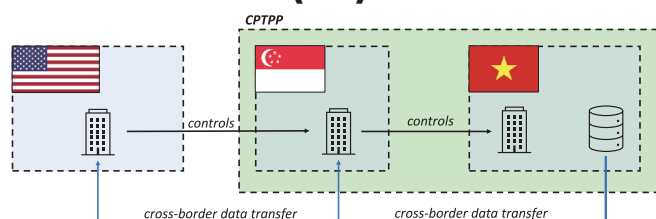
In this regard, the TPP's rules on cross-border data flows are more akin to investment protections for capital flows than to traditional trade rules for goods or services. For trade in goods, corporate nationality is immaterial because the status of the goods is determined based on territoriality: where did the goods come from? Similarly, for cross-border trade in services (mode 1 under GATS), territoriality, not corporate nationality, is decisive: is the service being provided from one territory to the other? The corporate nationality of the service supplier is also immaterial for consumption abroad (mode 2 under GATS) when a consumer of a certain nationality receives a service in another territory. Only when services are being supplied through commercial presence or presence of natural persons (modes 3 and 4 under GATS) in other territories, must the service supplier enjoy affiliation with a treaty party.

In contrast, investor status for purposes of investment protection under international investment law is largely determined by corporate nationality. By relying on this criterion for its provisions on cross-border data transfers and requirements to use domestic computing facilities, the TPP invites strategic incorporation by companies dependent on transnational ICT infrastructure. To illustrate how corporate multi-nationality affects the TPP model in practice, consider the case of a US company that owns and controls a subsidiary in Singapore which in turn owns and controls an entity in Vietnam. Even though the US has withdrawn from the TPP, the US company can still use its subsidiary under Singaporean law to claim that its Vietnamese entity must not be subjected to rules that would unduly restrict its cross-border data flows or would require it to use domestic computing facilities (*Chart 3*).

Importantly, under the TPP model, Vietnam is restricted from imposing undue restrictions on cross-border data flows vis-à-vis

CHART 3

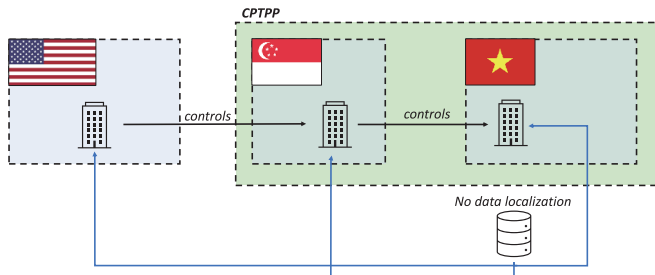
Multi-national corporation with cross-border data flows between a CPTPP member (Vietnam) and a non-CPTPP member (US)



Source: Compiled by the author

CHART 4

Multi-national corporation with ICT infrastructure outside CPTPP territory



Source: Compiled by the author

everyone, not just vis-à-vis Singapore (its treaty party) or the US (the home country of the corporate entity in question). In effect, under the TPP model companies may decide to locate their computing facilities *anywhere*. This is likely not an oversight but by design. Under the Silicon Valley Consensus, the preference is for companies, not governments, to determine how to use ICT infrastructure and where to locate it (Chart 4).

Countries might, of course, violate their commitments under the TPP model. Whether governments in this case will resort to state-state dispute settlement to force compliance remains to be seen. Countries committed to investor-state dispute settlement run the risk of being sued for damages if they unduly restrict cross-border transfers of information or mandate the use of domestic computing facilities. Aside from these formal mechanisms, businesses are likely to invoke the TPP model informally during investment negotiations or while lobbying for favorable regulations. In this way, the TPP model is a form of “meta-regulation” with the potential to indirectly shape policies in the digital domain by reinforcing and protecting the Internet’s infrastructural default for data flows irrespective of territorial boundaries.

Varieties of Data Localization

Why would countries restrict cross-border data transfers or require the use of domestic computing facilities in the first place? Extant scholarship on data localization tends to suggest that such restrictions or requirements are not necessary to achieve regulatory objectives such as data protection and cybersecurity. Framing the discussion around data localization in this way internalizes or presupposes the TPP model under which the necessity of such measures is a precondition for their legality.

I would like to suggest an alternative framing, which takes governments’ regulatory interest for data localization as its starting point rather than its end point. Under this alternative framing, data localization is not an end in itself or a means to an end but a way to establish effective jurisdictional control over data. The GDPR sets a default against cross-border transfers of personal information to ensure that data is being processed according to GDPR standards. If personal data is to be transferred from the EU to third countries, the EU insists on mechanisms that promise the continued protection of European subjects’ personal data. While the effectiveness and

compliance record of these mechanisms is disputed, they have certainly contributed to the global diffusion of European data protection and privacy standards.

China’s and India’s data localization requirements differ from the EU’s and ought to be evaluated on their own terms. In contrast to the EU which does not require the use of domestic computing facilities, China’s cybersecurity law requires “critical information infrastructure operators” to store “personal information” and “important data” within mainland China. Meanwhile, India is experimenting with data localization requirements meant to ensure that Indians’ personal data are collected and processed for the benefit of the Indian economy rather than others. All three jurisdictions are unlikely to commit to the TPP model any time soon, because its fundamental commitment towards free data flows is in tension with their evolving data governance frameworks.

The Osaka Track: a New Model

Writing in the *Japan SPOTLIGHT* May/June 2020 issue, Jota Ishikawa observed that rule-making for “digital trade” has lacked uniformity. This lack of uniformity might be as much an expression of divergent policy perspectives as the result of paralysis within international organizations. Meanwhile, the TPP model has been remarkably successful in attracting countries that are committed to the Silicon Valley Consensus while the GDPR has become a global model for data protection laws. In light of this disparate landscape, are there alternative models that could serve as templates for new rules on cross-border data flows under international economic law?

Abe proposed “Data Free Flow with Trust” (DFFT) at the January 2019 World Economic Forum in Davos and launched the Osaka track committed to this concept at the G20 summit in 2019. DFFT departs from the TPP model by requiring “trust” as a pre-condition for the free flow of data instead of assuming the free flow of data as an unconditional default that ought to be protected, in principle, from governmental regulations. DFFT raises many intricate questions: How to establish and maintain trust and between which entities – nation states, corporations, or citizens? Is the DFFT framework principally open for anyone to join or restricted to a “club” of like-minded nations? How does DFFT relate to established institutions, including the WTO and its efforts to craft multilateral rules for the digital economy? Is DFFT able to accommodate the EU’s framework of differentiated data protection while being compatible with the TPP model? All these questions will need to be worked out, if DFFT is to become a successful model for the regulation of cross-border data flows. In the meantime, the TPP model is likely to remain the most significant commitment towards free data flows and against data localization under existing international economic law.

JS

Thomas Streinz is executive director of Guarini Global Law & Tech and adjunct professor of Law at New York University School of Law.