THE RISE OF RESTRICTIONS ON DATA FLOWS AND DIGITAL TECHNOLOGIES: NATIONAL SECURITY, HUMAN RIGHTS, OR GEO-ECONOMICS?

This panel was convened at 12:30 p.m., Wednesday, March 24, 2021, by its moderator Thomas Streinz of Guarini Global Law & Tech, who introduced the panelists: Sarah Bauerle Danzman of Indiana University Bloomington; Yan Luo of Covington & Burling LLP; Maria Martin-Prat of the European Commission Directorate General for Trade; and George Mina, Australian Representative to the World Trade Organization.

Designing International Economic Data Law

doi:10.1017/amp.2021.102

*By Thomas Streinz**

For a second year in a row, the American Society of International Law had to convene an all virtual annual meeting because the COVID-19 pandemic made international travel and gathering in cavernous ballrooms impossible. I had the pleasure of chairing a pre-recorded panel on the rise of restrictions on data flows and digital technologies, which featured a stellar cast of experts distributed across three continents and time zones.[1] This panel depended on the digital infrastructure provided by a private videoconferencing company on top of the public infrastructure of interconnectivity that the internet has supplied for more than three decades. As the pandemic forced people around the world into lockdowns—albeit asynchronously and unevenly—it further mainstreamed the use of communications platforms for everyday interactions, whether public or private, whether for business or leisure.

In this and other ways, the pandemic revealed how reliant the global economy has become on digital data. Globally distributed networks of economic production have been enabled by information and communications technology (ICT) for which digital data is a medium through which information is being transmitted and shared transnationally. While companies have always relied on information to gain comparative advantage and have exploited information asymmetries accordingly, the use of "big data" promises new ways of gaining insight into business opportunities and market conditions within and across sectors. Public discourse is often dominated by concerns over global platform companies that generate vast amounts of personal data about their users in

* Adjunct Professor of Law and Executive Director of Guarini Global Law & Tech at New York University School of Law. While the views expressed in this Article are personal, my thinking about these issues has been heavily influenced by the Institute for International Law & Justice's MegaReg project with Benedict Kingsbury, Paul Mertenskötter, and Richard B. Stewart (www.iilj.org/megareg) and Guarini Global Law & Tech's Global Data Law project (www.guariniglobal.org/global-data-law) with Angelina Fisher and Benedict Kingsbury.

[1] The recording is publicly available on YouTube (May 26, 2021) at https://www.youtube.com/watch?v=xWN52rmDH8M&t=1s.

pursuit of information capitalist business models.[2] Yet, non-personal data such as industrial or environmental data can also be leveraged for commercial gain transnationally. Contemporary advances in artificial intelligence technology have enabled unprecedented image, audio, and text recognition and are routinely used to create, shape, and "optimize" algorithmically mediated spaces. These forms of machine learning depend crucially on very large datasets to train algorithms through "deep" neural networks.

For these reasons, the generation, commercial exploitation, and unhindered transnational transfer of data have become hallmarks of today's global digital economy. At the same time, deep digital divides persist and those who enjoy infrastructural control over the means of data production, not only attain de facto control over vast quantities of data but also determine qualitatively where and when what kind of data is being generated in what way and for what purpose.[3]

Concurrently with the digital transformation of economies and societies, transnational access, transfer, and use of data have increasingly become focal points during negotiations for "comprehensive" trade and investment agreements. While these efforts are often presented and discussed as negotiations about "electronic commerce" and "digital trade" that will "modernize" the *acquis* of international economic law, we are arguably witnessing the design of new international economic data law that is conceptually distinct from conventional international trade and investment law.

The design of this new international economic data law reflects a complex political economy. The world's largest trading blocs—the United States, the European Union, and China—have pursued different strategies and are now engaged in plurilateral negotiations on "electronic commerce" under the World Trade Organization's (WTO) plurilateral Joint Statement Initiative (JSI), which has attracted principal support from eighty-six WTO members, including all developed countries, but only five African countries and only three least developed countries.[4] Meanwhile, Singapore, New Zealand, and Chile have crafted new modular templates with the Digital Economic Partnership Agreement (DEPA), which showcases the range of digital governance issues (including artificial intelligence)[5] that instruments of international economic law can address, irrespective of a close nexus to traditional "trade" or "investment." These initiatives respond to demands for international rule-making in the digital domain. By using venues and instruments of international economic law, they shape the meta-regulatory frames within which domestic regulators and other norm setters craft new rules governing data and digital technologies. When our panel diagnosed and analyzed a "rise of restrictions," it implicitly acknowledged the absence of such restrictions as a default to be preserved rather than an ambition yet to be achieved. The internet affords a widespread, yet far from universal, ability for quasi-instantaneous transnational transmissions of data that departs from default parameters for which international economic law has historically been designed. Rather than enabling convergence in a world of regulatory divergence, international economic data law is designed to prevent such regulatory divergences from materializing by meta-regulating what and how governments can regulate in the digital domain.

[2] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (2019).

[3] Angelina Fisher & Thomas Streinz, *Confronting Data Inequality* (IILJ Working Paper 2021/1), *at* https://ssrn.com/abstract_id=3825724.

[4] Yasmin Ismail, *E-commerce in the World Trade Organization: History and Latest Developments in the Negotiations Under the Joint Statement*, Int'l Inst. Sustainable Dev. 14 (Jan. 2020).

[5] Shin-yi Peng, Ching-Fu Lin & Thomas Streinz, *Artificial Intelligence and International Economic Law: A Research and Policy Agenda*, *in* Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration 1, 18 (2021).

https://doi.org/10.1017/amp.2021.102 Published online by Cambridge University Press

To this end, the United States pioneered new provisions on cross-border data transfers and requirements to use domestic computing facilities in the original Trans-Pacific Partnership (TPP), and subsequently—despite its withdrawal from TPP—in the U.S.-Mexico-Canada Agreement (USMCA) and a dedicated "digital trade" agreement with Japan. These provisions require countries to not restrict the "free flow" of data (including personal data), unless there is a legitimate public policy objective that is being pursued in a non-arbitrary, non-discriminatory, or disguisedly trade restrictive manner and that does not impose greater restrictions than necessary to achieve the objective.[6] The resulting ability to transfer and store data transnationally is susceptible to regulatory arbitrage and de facto multilateralization due to the reliance on investment law categories which enable multinational corporations to benefit from these provisions even when their home jurisdiction is not or no longer a party to the agreement.[7] The U.S.-designed model inaugurated in TPP was endorsed by the remaining eleven countries that resurrected the agreement as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). It reflects a "Silicon Valley Consensus" that favors private sector interest in transnational data mobility by constraining states' ability to restrict and thereby regulate transnational "data flows."[8]

The European Union has been apprehensive about these kinds of commitments due to concerns that they might interfere with its General Data Protection Regulation (GDPR), which restricts cross-border transfers of personal data to third countries.[9] Initially, the EU took the position that the "free flow" of personal data was non-negotiable, because data protection and privacy are fundamental rights.[10] After lengthy internal deliberations that revealed tensions between the competent authorities within the European Commission, the EU presented a new template of horizontal provisions for cross-border data flows *and* for personal data protection in EU trade and investment agreements.[11] This template reconciles the competing interests by only restricting the data localization measures the EU does not deploy while protecting its data protection law from challenges. The EU has since tabled negotiation proposals reflecting this template in various negotiations, including the WTO's JSI initiative. However, the post-Brexit negotiations with the United Kingdom that culminated in the EU-UK Trade and Cooperation Agreement (TCA) revealed the limits of the EU's ability to turn its template into treaty law. The United Kingdom managed to downgrade data protection and privacy to mere rights (rather than fundamental rights) and to insert a novel commitment that ensures that instruments under conditions of general application (and not just entity by entity) are available to facilitate cross-border transfers of personal data.[12]

China long refrained from designing new international economic data law in its preferential trade and investment agreements.[13] Its intricate domestic data governance regime features various forms of data localization that not only restrict cross-border transfers of data, as the EU's GDPR does, but may indeed require not just territorial storage and processing but also local ownership over the relevant infrastructure. Yet, in November 2020, China signed the Regional and Comprehensive Economic Partnership (RCEP) agreement between the ASEAN countries and its trading partners,

[6] *See, e.g.*, Trans-Pacific Partnership, Arts. 14.11, 14.13.

[7] Thomas Streinz, *Data Governance in International Economic Law: Non-territoriality of Data and Multi-nationality of Corporations* (manuscript on file with author).

[8] Thomas Streinz, *Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy*, *in* MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP 312 (Benedict Kingsbury, et al. eds., 2019).

[9] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119/1, ch. V (May 5, 2016).

[10] EU Charter of Fundamental Rights, Arts. 7–8.

[11] The template is available at https://perma.cc/9R6Z-T7XW.

[12] EU-UK Trade and Cooperation Agreement, Art. 202.

[13] *See, e.g.*, Protocol to Upgrade the Free Trade Agreement Between the Government of the People's Republic of China and the Government of the Republic of Singapore, App. 6, new ch. 15.

https://doi.org/10.1017/amp.2021.102 Published online by Cambridge University Press

which created yet another model for international economic data law. Ostensibly modeled after TPP, RCEP echoes the principal commitment toward "free data flows" but grants much more leeway to countries to decide for themselves—rather than under external scrutiny—which restrictive measures *they* deem necessary.[14] Security-oriented measures, in particular, enjoy absolute protection.[15] To the surprise of some, China eventually if only belatedly also joined the WTO's JSI on electronic commerce, where it has advanced a relatively narrow conception of "electronic commerce" that focuses on Internet enabled trade in goods and related payment and logistics services. In line with RCEP's model, China consistently pushes for strong exceptions to guarantee cybersecurity and to safeguard "cyberspace sovereignty."[16]

Due to their different approaches to internal and external data governance that are also reflected in their submissions to the JSI, the United States, the European Union, and China are often portrayed as distinct "data realms" with different approaches to global data ordering.[17] In this narrative, the United States advances the "Silicon Valley Consensus" favored by its dominant platform companies; the European Union pursues a stringent regulatory agenda gravitating around the GDPR's protections of personal data as fundamental rights; and China maintains the legal-infrastructural protections of its "Great Firewall" which caters to authoritarian security interest as well as protectionist economic interests. While there is some truth to this narrative, designing new international economic data law may require a more nuanced and more complex account. While it is true that the United States championed an agenda of "internet freedom" since the 1990s, its restrictive measures leveled against Chinese telecommunications infrastructure (Huawei) and social media platform providers (Tencent's WeChat and ByteDance's TikTok) illustrate that its erstwhile and principal commitment to "free data flows" is contingent and certainly not absolute.[18] While the GDPR remains at the heart of its supranational data law, the EU is crafting a broader array of regulatory instruments recalibrating data relations. These initiatives are not focused on protecting Europeans' fundamental rights but seek to achieve a European version of "digital sovereignty" to regain regulatory control and to jumpstart the lagging European digital economy. Meanwhile, China is creating sophisticated data governance frameworks that often incorporate concepts from European data law. As the Chinese Communist Party seems keen on reigning in its powerful technology companies domestically, these same companies continue to play important roles in its 'Digital Silk Road' strategy which shapes data governance regimes abroad, especially in Central Asia, Latin America, and Africa, by supplying digital infrastructure.[19]

The United States, the European Union, and China—in distinctive yet sometimes functionally comparable ways—have exercised considerable influence over the digital destinies of people around the world. Designing new international economic data law is but one and certainly not the most important lever of influence. However, policymakers and civil society in other countries must be aware that long-lasting meta-regulatory frameworks are being created which may not cater

[14] Thomas Streinz, *RCEP's Contribution to Global Data Governance*, AfronomicsLaw (Feb. 19, 2021), *available at* https://perma.cc/HQJ4-QN42.

[15] *See* Regional and Comprehensive Economic Partnership, Arts. 12.14, 12.15.

[16] Henry Gao, *Across the Great Wall: E-commerce Joint Statement Initiative Negotiation and China*, *in* Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration 295, 310 (Shin-yi Peng, Ching-Fu Lin & Thomas Streinz eds., 2021).

[17] *See, e.g.*, Susan Aariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. Int'l Econ. L. 245 (2018).

[18] *See also* Sarah Bauerle Danzman, *National Security, Investment Review, and Sensitive Data*, 115 ASIL Proc. __ (2021).

[19] Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 N.Y.U J. Int'l L. & Pol. __ (forthcoming 2021), *available at* https://ssrn.com/abstract=3810256.

https://doi.org/10.1017/amp.2021.102 Published online by Cambridge University Press

to the rights, interests, and needs of the diverse publics they represent and serve. The design of new international economic data law also presents an opportunity for other countries to challenge digital hegemony and to develop alternative proposals. India, which pursues a digital industrial policy in tension with the anti-protectionism consensus enshrined in international economic law, and South Africa, which is involved in the African Union's digital transformation strategy for Africa that emphasizes digital sovereignty, have challenged the legitimacy and legal status of the WTO's JSI.[20] The negotiations for a protocol on electronic commerce to be added to the African Continental Free Trade Area (AfCFTA) may be an opportunity to develop an African approach toward international economic data law outside the WTO.

If the WTO fails to engineer a compromise between its members that participate in the JSI on "electronic commerce," attention and political support for designing new international economic data law will likely shift toward bilateral and regional digital economy agreements (either standalone or as part of "comprehensive" trade and investment agreements). Such efforts will continue simultaneously and in continuous correspondence with domestic data regulation, which can have significant transnational implications, as the EU's GDPR demonstrates.[21] Private sector dominated standard-setting organizations play outsized and expanding roles in the digital domain, which may require a reckoning with how their activities interface with domestic law and international economic law. To retain relevance and to contribute to human flourishing, the designers of new international economic data law may need to switch focus. Rather than leveraging hard to change and even harder to leave treaty commitments to meta-regulate if, when, and how countries can regulate and thereby self-determine their transition toward digitally mediated societies and economies, international economic data law should focus on facilitating interoperability between different data governance approaches without imposing uniformity. This kind of international economic data law would allow for experimentation and flexibility while retaining compatibility and accepting a certain degree of uncertainty.

In any case, as international economic law expands its remit to encompass a broad array of data governance questions, its substance and design process warrant critical scrutiny. When designing new international economic data law, one must ask which issues to address or prioritize and whose interests are being served: Are novel restrictions imposed by governments the most pressing issue or might quasi-monopolistic infrastructural control over "data flows" by platform companies warrant more attention? Is the traditional separation of trade and tax sustainable when sophisticated tax avoidance schemes deprive governments of the public funds they might need to build critical digital infrastructure or to support those who are adversely affected as their lives become increasingly datafied and algorithmically governed? Can international economic data law be designed to encourage mitigation of the significant greenhouse gas emissions caused by energy-hungry data centers? Finding answers to these and many other questions requires rigorous public debate within and across countries and institutions, robust civil society involvement, and reliable data. Unfortunately, the venues in which international economic data law is being designed tend to operate as if these were conventional trade negotiations in which offensive and defensive interests are being traded off by adjusting market access commitments or tariff schedules. To gain (rather than assume) institutional legitimacy, the design of international economic data law must be more transparent and participatory in ways that help equalize power imbalances. While the fear that opening up the design process in this way might complicate or derail negotiations is understandable, this is a challenge to be embraced rather than a problem to be avoided. As the Paris Climate Agreement

[20] WTO General Council, The Legal Status of "Joint Statement Initiatives" and Their Negotiated Outcomes, WTO Doc. WT/GC/W/819 (Feb. 19, 2021).

[21] Anu Bradford, The Brussels Effect: How the European Union Rules the World, ch. 5 (2020).

https://doi.org/10.1017/amp.2021.102 Published online by Cambridge University Press

shows, there is considerable potential in facilitating new transnational coalitions involving governments, companies, and civil society organization that can push together for desirable political outcomes, including a better international economic data law. To assess the impact of any such rule-making effort, the persistent and paradoxical lack of data about state of the global digital economy ought to be addressed, if necessary by mandating data disclosures from those who control large-scale data generating infrastructures for statistical purposes.

Neither our panel nor this introductory essay could address all these important questions and rough ideas in depth. But raising them is a first step to design better international economic data law in future.

National Security, Investment Review, and Sensitive Data

doi:10.1017/amp.2021.103

*By Sarah Bauerle Danzman**

As a scholar of the politics of the nexus of national security and investment policy, I can best add to the discussion on the issue of data and digital tech restrictions mostly from a foreign investment regulation and investment screening vantage point.

The politics of investment review for national security purposes points to three central issues. First, a growing number of high-income countries increasingly view large volumes of consumer data as a potential vulnerability that threat actors can exploit. While Europe has been a leader on stricter data privacy regulation, the United States has arguably the most assertive position on screening foreign investment acquisitions for national security concerns arising from sensitive personal data. This is clear from the very public dispute over ByteDance's ownership of TikTok[1] and also reporting in the news that the U.S. screening mechanism—the Committee on Foreign Investment in the United States (CFIUS)—required a Chinese business to divest from the gay dating app, Grindr, in 2019.[2] But many other advanced economies are expanding their screening authorities to also include data privacy issues.[3] So, we should not see this as a purely American phenomenon.

Second, sensitive personal data can create multiple national security concerns that governments must contend with. At the most basic level, when foreign firms own and control large amounts of personally identifying and sensitive information on domestic persons, host countries may face legitimate concerns that the foreign firms' government may be able to gain access to those data repositories for intelligence purposes. Governments may be especially wary if there is a lack of trust as to whether the foreign business that controls access to sensitive personal data will protect it from authorities or share it with their home country government if asked or demanded to do so. Third, host countries are frequently worried that many businesses in the digital era have the capacity to engage in targeted data collection may be used to collect sensitive information that borders on intelligence such as troop movements or the activities of diplomats, or used to blackmail or recruit

* Assistant Professor of international studies at Indiana University Bloomington.

[1] Echo Wang & David Shepardson, *China's ByteDance Challenges Trump's TikTok Divestiture Order,* Reuters (Nov. 11, 2020), *at* https://www.reuters.com/article/usa-tiktok/chinas-bytedance-challenges-trumps-tiktok-divestiture-order-idUSKBN27R07W.

[2] Carl O'Donnell, Liana B. Baker & Echo Wang, *Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, Reuters (Mar. 27, 2019), *at* https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-told-u-s-security-at-risk-chinese-firm-seeks-to-sell-grindr-dating-app-idUSKCN1R809L.

[3] Sarah Bauerle Danzman & Sophie Meunier, *The Big Screen: Global Crises and the Diffusion of Foreign Investment Review* (unpublished manuscript, on file with author).