CGD BRIEF
AUGUST 2021

Do Evolving Digital Trade Rules Create an Uneven Playing Field? Understanding Global Perspectives

Roundtable Summary

Compiled by Michael Pisa and Ugonma Nwankwo

INTRODUCTION

When national data policies are harmonized, organizations can more easily participate in the global digital economy. But the process of harmonization is inherently political, as it involves countries aligning their domestic practices with a single set of standards and principles. Reflecting the asymmetry of power in the global digital economy, the data governance choices made by a handful of jurisdictions—particularly, the European Union, United States, and, increasingly, China—strongly influence the set of policy options available to other countries. These major powers promote their digital policies abroad through trade agreements and mechanisms to establish the legality of cross-border data flows, including "adequacy" determinations.

This meeting is the second in a series of private roundtables convened by the Center for Global Development aimed at exploring the relationship between data governance and economic development. The first roundtable, held on May 20, 2021, examined whether current approaches to data protection and privacy are a good fit for resource-constrained countries. This second roundtable explored whether current trade dynamics provide countries enough flexibility to enact policies that meet their own needs and priorities and whether they support or hinder economic development.

This document summarizes key takeaways from the meeting, including the remarks of three keynote speakers and themes raised in a discussion among 30 experts, who are listed in the appendix. The roundtable was moderated by Pam Dixon, founder and executive director of the World Privacy Forum, and co-chair of the working group for CGD's Governing Data for Development project. Because we aim to summarize the discussion faithfully, we provide additional context only when it is necessary to help readers understand the points raised.

KEY TAKEAWAYS

Through the course of the roundtable, a handful of key themes emerged from the dialogue. These themes are summarized below.

The fraught relationship between privacy and trade policy

- Trade agreements are the dominant mechanism for aligning digital policies across countries but

This brief is based on a roundtable hosted by CGD as part of the Governing Data for Development project, which explores how governments can use data to support innovation, development, and inclusive growth while protecting citizens and communities against harm. The views expressed here are those of the participants and do not necessarily represent the views of CGD staff. For other briefs in the series, as well as more on the project, visit cgdev.org/governing-data.

are ill-equipped to handle the multifaceted nature of data. Participants emphasized the need for trade agreements to evolve in a manner consistent with a rights-based approach to data privacy.

The politicization of GDPR adequacy

- Many participants viewed the European Commission's approach to determining GDPR adequacy as driven by political and economic considerations, rather than the fitness of a country's data protection regime. The opacity of the adequacy process exacerbates this perspective.

- The EU can instill greater trust in the process—and set a better example for other countries to follow—by being more transparent about how adequacy decisions are reached, including publicly stating why decisions are denied or delayed for certain countries.

Defragmenting the data policy landscape

- Inconsistent digital policies pose a barrier to competition and a hurdle for countries seeking to develop their own digital economy. Harmonizing national data rules would promote cross-border economic activity and benefit smaller companies that lack the legal teams needed to navigate different regulatory environments.

- While many participants believed that a global agreement on data privacy and protection standards would be the best solution, they doubted whether achieving it is possible given current institutional arrangements and political dynamics. Instead, the group sketched out an alternative path forward that relies on regional harmonization and a sectoral approach to achieving adequacy.

KEYNOTE REMARKS

The roundtable opened with three keynote presentations. The following are summaries of the remarks made by Melissa Omino (research manager, Center for Intellectual Property and Information Technology Law, Strathmore University), Eduardo Bertoni (representative of the Regional Office for South America, Inter American Institute of Human Rights and former director, Data Protection and Access to Information Authority of Argentina), and Deborah Elms (founder and executive director, Asian Trade Centre).

Summary of remarks by Melissa Omino, Center for Intellectual Property and Information Technology Law, Strathmore University

Current trade dynamics undermine the ability of countries to enact digital governance policies that meet their own needs and priorities. This is especially true in developing countries due to power imbalances in trade negotiations. An example in sub-Saharan Africa is the US-Kenya Free Trade Agreement currently under negotiation.

Negotiations of the US-Kenya FTA were first made public in early 2020, when both countries published their objectives for an agreement. The US has three objectives relating to cross border data flows:

1. To prevent Kenya from imposing measures that restrict these flows, including by requiring the use or installation of local computing facilities

2. To promote the interoperability of data protection regimes and mechanisms to facilitate cross-border transfers

3. To establish rules that prevent the government from mandating the disclosure of computer source code algorithms

Kenya's overarching objective on digital trade is to obtain a "secure commitment to allow gradual regulations at facilitation of digital trade in goods and services and cross-border data flow in line with the [country's] development agenda, in particular, contribution of this trade to economic development." Compared to the US' clearly defined objectives, this goal is vague and difficult to understand.

Kenya is a data exporter (i.e., more data flows out of the country than into it) so, unfettered cross-border data flows would likely benefit US-based data-driven companies more than Kenyan ones. Weakly regulated cross-border data flows would also raise concerns about how commercial data pertaining to Kenyans (including data collected through Vodafone's mobile money service M-Pesa) could be used by companies abroad.

The data protection landscape in Kenya is still nascent, as its Data Protection Act (DPA) was only enacted in 2019. Although still evolving, Kenya's DPA requires proof of adequate data protection safeguards in the destination country as a prerequisite to cross-border data transfers. US negotiation objectives would prevent the Kenyan government from carrying out this legal requirement.

Human rights, including the right to privacy, rarely take precedence within the realm of trade. Nevertheless, the fact that much of the data that flows across borders is personal data means that the right to privacy must be at the forefront of policy discussions on cross-border data flows.

Nigeria has recently sought to introduce developing country exceptions into the ongoing WTO e-commerce agreement talks that would exempt low-income countries from data-related obligations. This would be a step in the right direction for sub-Saharan Africa within the WTO.

We support using open data, public domain data, or data held by the government that does not impact a person's privacy to create solutions for Africa. But we must recognize that most of this data is processed outside of Africa, which means that value-added innovation takes place elsewhere and often fails to benefit those who contributed their data in the first place.

Summary of remarks by Eduardo Bertoni, Regional Office for South America of the Inter American Institute of Human Rights

To what extent does having harmonized data laws, particularly laws related to cross-border data flows, affect economic development? Many people assume that having flexible norms and regulations that support the free flow of data will increase economic activity and development. I have the same intuition, but I have yet to see an empirical study to back up this assumption. For the moment, however, let us assume that greater coordination in support of free-flowing data is beneficial.

What is the best strategy to harmonize laws to allow data to flow easily across borders? I will speak to the Latin American experience, which is heterogeneous because of the region's diversity. The relationships Latin American countries have with major economic powers strongly influence how they approach digital trade policy. This helps explain differences in how deeply the "Brussels effect" has influenced Latin American countries.

For example, much of Argentina and Uruguay's foreign commerce is conducted with the EU, so it is important for these countries to be aligned with the GDPR (they are the only two countries in Latin America deemed "adequate" by the European Commission to date). Contrarily, Colombia and Mexico conduct most of their foreign commerce with the United States. While receiving an adequacy determination would make it easier for their companies to conduct business with the EU (the Mexican government has expressed interest in achieving adequacy), it is economically important for these countries to align with US data policies.

Countries that want to achieve GDPR adequacy often view joining the Council of Europe's Convention 108 and its successor *Convention 108+* (the only legally binding international agreement on data protection standards) as important stepping stones. Three Latin American countries are already members of Convention 108 (Argentina, Mexico, and Uruguay), while several others have expressed interest in joining. Despite this, there is a perception among some Latin American policymakers that the Council of Europe and the EU are promoting their standards on other countries. There is also a perception that the EU has been more accommodating in adequacy negotiations with rich countries while remaining inflexible with low-and middle-income countries.

Latin American nations are often caught in between the United States and EU on data policy. Meanwhile, China is playing an increasingly important economic role in the region, complicating matters for Latin American governments. For example, Argentina wants to have a strong relationship with the EU but does not want to be considered a country unable to conduct business with the US or China.

Having a global agreement on data protection standards would help to address this challenge. It is unclear, however, whether achieving such an agreement through a body like the United Nations is possible, or if other strategies should be explored. In the absence of a global agreement, the most likely outcome is a patchwork of

bilateral and multilateral agreements. This would be a disaster for companies and countries.

Lastly, it is important to consider the role of personal data transfers in conducting criminal investigations and combatting cybercrime. The Budapest Convention is a good agreement that allows law enforcement authorities to exchange information, including personal data, to support their investigations. But the process to update the Convention has been politically fraught, particularly on the data protection chapter where law enforcement agencies want to include surveillance and AI approaches—two high-risk areas where the US and EU have different preferences.

Summary of remarks by Deborah Elms, Asian Trade Centre

Asia is a diverse region with diverse views on how to conduct digital policy. While a few governments continue to impose comprehensive restrictions on cross-border data flows, the overall trend is towards greater cooperation and harmonization to foster more digital trade in the region.

One of the biggest challenges in the digital policy space from a development perspective is regulatory incoherence. Regulations do not have to be identical, but they should have the same general objective and be aligned where possible. Otherwise, conducting business across borders is difficult, especially for smaller companies. The region has used different approaches to achieve this alignment, including incorporating e-commerce chapters into traditional trade agreements and creating novel digital-only trade agreements.

Traditional trade agreements. Both of Asia's newest regional trade agreements, the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTTP) include e-commerce chapters that create binding multilateral rules related to cross-border data flows, data localization, intellectual property rights in the digital space, and the digital delivery of services (including financial services). Of the two, the CPTPP—which was signed by 11 countries in 2018 after the United States withdrew from the Trans-Pacific Partnership negotiations—has more expansive and rigid rules on digital trade, while the RCEP provides its members with significant leeway to enact restrictive measures on data flows and the location of computational facilities.[1]

ASEAN is working to implement the Agreement on E-Commerce signed in 2018, which seeks to harmonize data policies across the region with the long-term aim of creating a digital single market. ASEAN member governments tend to be enthusiastic about broad and ambitious digital commitments because they recognize the power of the digital economy to help their businesses, including small businesses.

Digital-only trading agreements. Several countries in the region have taken a more novel approach, using Digital Economy Agreements (DEAs), which countries can "dock into" their existing free trade agreements, usually by replacing existing e-commerce chapters to modernize their approach to digital trade while relying on the soft infrastructure that underlies trade agreements, including mechanisms for dispute settlement. DEAs also often incorporate non-binding MOUs that cover different topics viewed as relevant but where national policy approaches do not yet exist (e.g., artificial intelligence and big data).

The Digital Economy Partnership Agreement (DEPA), which Singapore, New Zealand, and Chile signed in 2020, is the first stand-alone digital-only trade agreement. DEPA takes a modular approach to digital trade issues, with 12 different modules for different areas including data flows, trust environment, digital identities, and digital inclusion. Countries can either sign onto the entire agreement or select specific modules and dock them into existing trade agreements.

Joint Statement Initiatives (JSIs) on e-commerce, which allow WTO members to begin negotiations on digital trade issues without adhering to the rule of consensus decision-making, are also growing in popularity in Asia and globally. JSIs aim to support the predictable alignment of rules related to e-commerce, including online delivery, data flows, data localization, and digital payments.

1 CPTPP, which was signed in 2018, has 11 member states, including Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam. RCEP, which was signed in 2020, has 15 members states, including all 10 members of ASEAN plus China, Japan, Korea, Australia, and New Zealand.

ROUNDTABLE DISCUSSION

The keynote remarks were followed by a moderated discussion focused on questions and issues raised by the opening speakers. The following are key themes that emerged from this discussion.

The fraught relationship between privacy and trade policy

There was a lively debate on whether trade agreements are appropriate instruments for aligning national data and digital policies.

Several participants argued that data privacy should be conceived first and foremost as a human right and kept separate from trade policy discussions whenever possible to avoid watering down data privacy rules. They believed that seeking alignment on digital policies through trade agreements would bias them in favor of promoting commerce and against protecting privacy, which would ultimately create greater public distrust in data use.

Others argued that trade agreements are ill-equipped to resolve challenges raised by the multifaceted nature of data, which makes them fundamentally different than traditional goods and services. Because rules on cross-border data flows strongly influence how governments manage politically and socially sensitive issues related to data privacy, law enforcement, national security, and cybercrime, national governments should enforce policies that reflect the values of the society they represent. For that reason, one participant argued that countries should seek agreement on a common stance towards data privacy and protection *before* starting digital trade negotiations. Bilateral trade agreements were seen as disadvantageous for low- and middle-income countries because they mirror and perpetuate power imbalances in favor of Big Tech companies.

Countering these reservations, several participants argued that including digital issues in trade agreements is both crucial and inevitable as economies become increasingly digital. The cost to companies of being unable to participate in the global digital economy is too high for digital issues not to be included in trade agreements. They argued that trade agreements were a useful mechanism for achieving greater alignment of digital policies because frameworks for negotiation already exist.

The politicization of GDPR adequacy

The EU's GDPR adequacy process is the means through which the European Commission determines whether non-EU countries "provide a level of protection for personal data which is comparable to those of EU law" as the basis for transferring data.[2] Roundtable participants agreed that countries should have the right to assess whether their citizens' data will be handled responsibly by organizations in other countries before allowing that data to be shared across borders. But several expressed frustration with how the European Commission has managed the GDPR adequacy process, arguing that it has been opaque and unfair.

Several participants noted that the European Commission's approach to determining adequacy appeared to be driven by political and economic considerations rather than the fitness of a country's data protection regime. As an example, one participant highlighted how the European Commission granted Japan adequacy in 2019 despite key differences between the GDPR and Japan's model of cooperative data privacy, while also delaying making decisions on the adequacy of countries whose rules are similar to the GDPR, including Argentina and Uruguay.[3]

One participant highlighted the European Commissions' pursuit of a deal with the United States to resolve uncertainty around transatlantic data flows in the wake of the Schrems II case as another example of how the Commission seemed to apply data privacy standards differently depending on the economic heft of its trading partners.[4] Another participant argued that economic aims should not drive decisions on data privacy standards, nor should data privacy standards be used as a "cover" for furthering economic policy.

2 https://gdpr-info.eu/issues/third-countries/.

3 A review of the Adequacy decision for Japan notes that "the Adequacy Decision is…significant for illustrating the limited success of the European Union's vision of utilizing the GDPR to establish global human rights standards." (Flora Wang, Harvard Journal of Law & Technology, 2020).

4 [Schrems II, the decision by the Court of Justice of the European Union in July 2020 to declare "the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programmes].

According to participants, the perception that the EU has implemented GDPR adequacy inconsistently is exacerbated by the opacity of the adequacy determination process. Several complained that there is no standardized approach for determining adequacy. One participant suggested that the EU can instill greater trust in the process—and set a better example for other countries to follow—by being more transparent about how adequacy decisions are reached, including publicly stating why decisions are denied or delayed for certain countries.

More broadly, participants expressed wariness about how well a GDPR-like framework could work outside of Europe. One participant noted that policymakers in Asia are skeptical of whether the rules and standards created to work in the European context could also work in more diverse and less institutionally integrated parts of the world.

Defragmenting the data policy landscape

Despite most participants' skepticism of trade agreements as the best means to promote alignment of digital policies, there was broad agreement on the value of having more consistent rules on data and digital tools across countries. At the same time, several participants emphasized that promoting cross-border data flows should not be mistaken for an end in itself and should be pursued only when consistent with a human rights approach to data privacy.

While the existing patchwork of digital regulations makes it harder for all companies to operate across borders, it particularly disadvantages smaller companies since they lack the legal teams needed to navigate different regulatory environments. As such, inconsistent digital policies pose a barrier to competition and a hurdle for countries seeking to develop their own digital economy.

Several participants warned that a profusion of national data protection adequacy regimes would increase fragmentation *unless* they are based upon similar standards and a similar interpretation of those standards. One participant argued that if too many African countries follow Kenya in enacting their own adequacy process for cross-border data sharing, it could complicate efforts to promote free trade and e-commerce in the region.

While many participants believed that a global agreement on data privacy and protection standards would be the best solution, they also doubted whether achieving it is possible given current institutional arrangements and political dynamics. Instead, the group sketched out a path forward that could deliver a second-best outcome through regional harmonization and a sectoral approach to achieving adequacy.

The conversation focused on three potential benefits of greater regional harmonization: (1) promoting economic activity by removing barriers to cross-border trade and investment; (2) strengthening the protection of data by facilitating cross-border cooperation between regulators and data protection authorities; and (3) boosting the negotiating power of smaller countries vis-à-vis larger ones by creating blocs of countries with aligned standards.

In addition, one participant argued that adequacy exercises would be easier to conduct (and easier for applying countries to prepare for) if they were narrower in scope—focusing on types of data according to use or sector, rather than the entire data protection regime within a country. This would allow governments to modernize their data privacy regimes sequentially and according to the value and risk attached to using data in certain sectors, while drawing on the expertise housed in sectoral regulatory agencies.

Conflicting views on data localization

It is increasingly common for data protection regimes to include localization measures that require firms who collect data about a country's citizens to store or process that data within the same jurisdiction. Most recently, Sri Lanka, Pakistan, Bangladesh, and India have drafted data protection rules that include localization measures. Several participants argued that these measures create costs for local companies and are generally ineffective. Others highlighted the importance of keeping certain types of sensitive data, including election data, on local servers.

One participant noted that, while politicians often like the idea of restricting the movement of data produced in their jurisdictions—and often do so for law enforcement reasons—most local companies oppose such restrictions because they prevent them from using foreign cloud

providers that can deliver higher quality and more secure data storage options than domestic ones.

Another participant noted that before enacting data localization measures, policymakers should have sustained conversations with local data-driven businesses about how they use data and how proposed reforms would affect them. Too often, policymakers (and digital policy experts) do not understand how data moves on the internet, which leads to the creation of rules and regulations that either cannot be implemented or would undermine prospects for development.

Finally, one participant argued that incorporating localization measures into data protection laws undermines the foundational principles of the data protection movement (including the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which forms the basis of most modern privacy laws), which sought to protect personal data and promote the flow of data across borders with appropriate safeguards.

NEXT STEPS

This event was the second in a series of private roundtables that the Center for Global Development is hosting to explore the relationship between data governance and economic development. A subsequent roundtable will explore how global and regional institutions can support better data governance practices and ways to increase the input of low- and lower-middle income countries into debates on the design of global data governance standards.

The insights shared in the roundtable discussions will inform CGD's Governing Data for Development Working Group in drafting recommendations on steps policymakers can take at the regional and global levels to support the creation and implementation of data policies that work well for all countries. More information on the project, including a series of blogs and other roundtables summaries can be found here.

ROUNDTABLE PARTICIPANTS

Abebe Shimeles, African Economic Research Consortium

Adedeji Adeniran, Centre for the Study of the Economies of Africa

Aretha Mare, Smart Africa

Ashnah Kalemera, Collaboration on International ICT Policy in East and Southern Africa

Burcu Kilic, Public Citizen

Deborah Elms, Asian Trade Centre

Deepa Karthykeyan, Athena Infonomics

Dianah Ngui Muchai, African Economic Research Consortium

Dimuthu Attanayake, LirneAsia

Drudeisha Madhub, Data Protection Office of Mauritius

Eduardo Bertoni, Inter-American Institute of Human Rights (IIDH)

Fabrizio Scrollini, Open Data Latin American Initiative

Flor Serale, The Open Data Institute

Henriette Cyuzuzo, Smart Africa

Helani Galpaya, LirneAsia

Isaac Rutenberg, The Centre for Intellectual Property and Information Technology Law

Martina Barbero, Global Partnership for Sustainable Development Data

Martine Julsaint Kidane, United Nations Conference on Trade and Development

Melissa Omino, The Centre for Intellectual Property and Information Technology Law

Pilar Fajarnes Garces, United Nations Conference on Trade and Development

Rachel Sibande, UN DIAL

Rohan Samarajiva, LirneAsia

Sone Osakwe, Centre for the Study of the Economies of Africa

Sunday Morabu, UN DIAL

Susan Aaronson, Digital Trade and Data Governance Hub

Tanvir Singh Natt, UN DIAL

Teki Falconer Akuetteh, Africa Digital Rights Hub

Thelma Quaye, Smart Africa

Torbjörn Fredriksson, United Nations Conference on Trade and Development

Victor Ndede, Amnesty Kenya

Center for Global Development
Ideas to Action: Independent research for global prosperity

WWW.CGDEV.ORG

MICHAEL PISA is a policy fellow at the Center for Global Development.

UGONMA NWANKWO is a research assistant at the Center for Global Development.