234 Research Paper
29 May 2026

The Digital Trade Data Heist: Trade Agreement Limits on Data Transfer and Storage Regulation Could Undercut Data Governance

Daniel Rangel, Jai Vipra and Lori Wallach

SOUTH CENTRE

RESEARCH PAPER

234

THE DIGITAL TRADE DATA HEIST: TRADE AGREEMENT LIMITS ON DATA TRANSFER AND STORAGE REGULATION COULD UNDERCUT DATA GOVERNANCE[1]

Daniel Rangel, Jai Vipra, and Lori Wallach[2]

SOUTH CENTRE

29 MAY 2026

[1] An earlier version of this paper was circulated through Rethink Trade's *Digital Trade Briefing Papers Series.* The paper submitted to the South Centre was finalized in January 2026.

[2] Daniel Rangel is Research Director of the Rethink Trade program at the American Economic Liberties Project. Jai Vipra is an AI policy and digital governance researcher. Lori Wallach is the Director of the Rethink Trade program at the American Economic Liberties Project.

SOUTH CENTRE

In August 1995, the South Centre was established as a permanent intergovernmental organization. It is composed of and accountable to developing country Member States. It conducts policy-oriented research on key policy development issues and supports developing countries to effectively participate in international negotiating processes that are relevant to the achievement of the Sustainable Development Goals (SDGs). The Centre also provides technical assistance and capacity building in areas covered by its work program. On the understanding that achieving the SDGs, particularly poverty eradication, requires national policies and an international regime that supports and does not undermine development efforts, the Centre promotes the unity of the South while recognizing the diversity of national interests and priorities.

NOTE

The views contained in this paper are attributable to the author/s and do not represent the institutional views of the South Centre or its Member States. Any mistake or omission in this study is the sole responsibility of the author/s.

Any comments on this paper or the content of this paper will be highly appreciated. Please contact:

South Centre
International Environment House 2
Chemin de Balexert 7–9
1219 Geneva
Switzerland
Tel. (41) 022 791 80 50
south@southcentre.int
www.southcentre.int

ABSTRACT

Governments worldwide are increasingly regulating how data is collected, transferred and stored to advance public interest objectives, including privacy, national security, taxation of the digital economy, and competition in the emerging artificial intelligence (AI) field. However, recent "digital trade" rules in international agreements — particularly those modeled on the United States–Mexico–Canada Agreement (USMCA) — restrict governments' ability to regulate cross-border data flows or to require local data storage. This paper analyzes the expanding divergence between domestic data-governance measures and binding trade commitments. It evaluates three major models of digital trade rules (USMCA, Mercosur (*Mercado Común del Sur*), and European Union–New Zealand) and demonstrates that the USMCA framework imposes the most sweeping constraints and the weakest exceptions. The analysis also shows that such trade rules may hinder broader regulatory efforts related to taxation and AI accountability.

Partout dans le monde, les gouvernements réglementent de plus en plus la collecte, le transfert et le stockage des données afin de promouvoir des objectifs d'intérêt public, notamment la protection de la vie privée, la sécurité nationale, la fiscalité de l'économie numérique et la concurrence dans le domaine émergent de l'intelligence artificielle (IA). Cependant, les récentes règles relatives au « commerce numérique » figurant dans les accords internationaux — en particulier celles inspirées de l'Accord États-Unis-Mexique-Canada (l'USMCA) — limitent la capacité des gouvernements à réglementer les flux transfrontaliers de données ou à exiger le stockage local des données. Le présent document analyse la divergence croissante entre les mesures nationales de gouvernance des données et les engagements commerciaux contraignants. Il évalue trois grands modèles de règles en matière de commerce numérique (l'Accord États-Unis-Mexique-Canada, Mercosur (Mercado Común del Sur) *et Union européenne-Nouvelle-Zélande) et démontre que le cadre de l'USMCA impose les contraintes les plus radicales et les exceptions les plus limitées. L'analyse montre également que de telles règles commerciales peuvent entraver des efforts réglementaires plus larges liés à la fiscalité et à la responsabilité en matière d'IA.*

Los gobiernos de todo el mundo están regulando cada vez más la forma en que se recopilan, transfieren y almacenan los datos para promover objetivos de interés público, entre los que se incluyen la privacidad, la seguridad nacional, la fiscalidad de la economía digital y la competencia en el campo emergente de la inteligencia artificial (IA). Sin embargo, las recientes normas sobre «comercio digital» incluidas en los acuerdos internacionales —en particular, las inspiradas en el Acuerdo Estados Unidos-México-Canadá (USMCA)— limitan la capacidad de los gobiernos para regular los flujos transfronterizos de datos o exigir su almacenamiento local. Este documento analiza la creciente divergencia entre las medidas nacionales de gobernanza de datos y los compromisos comerciales vinculantes. Evalúa tres modelos principales de normas de comercio digital (USMCA, Mercosur [Mercado Común del Sur] y Unión Europea-Nueva Zelanda) y demuestra que el marco del USMCA impone las restricciones más amplias y las excepciones más débiles. El análisis también muestra que dichas normas comerciales pueden obstaculizar los esfuerzos regulatorios más amplios en materia de fiscalidad y la rendición de cuentas en materia de IA.

全球各国政府正日益加强对数据收集、传输和存储方式的监管，以推进公共利益目标，包括隐私保护、国家安全、数字经济征税以及新兴人工智能（AI）领域的竞争。然而，国际协议中近期的“数字贸易”规则——尤其是那些以《美墨加协定》（USMCA）为蓝本的规则——限制了各国政府监管跨境数据流动或要求本地数据存储的能力。本文分析了国内数据治理措施与具有约束力的贸易承诺之间日益扩大的分歧。文章评估了三种主要的数字贸易规则模式（美墨加协定、南方共同市场（Mercosur）以及欧盟-新西兰协定），并指出美墨加协定框架施加的限制最为广泛，而例外条款却最为薄弱。分析还表明，此类贸易规则可能会阻碍与税收及人工智能问责制相关的更广泛监管努力。

TABLE OF CONTENTS

INTRODUCTION

Data flows. Every time we send an email, stream a video, or access an online document, data is flowing, potentially across borders. Information has been flowing internationally, through submarine cables and satellites, for decades now. The movement of data supports an array of important policy goals, including the functioning of the World Wide Web. However, recognizing the importance of the international flow of information is not the same as forbidding policies that ensure the movement of data does no harm to, and indeed furthers, public interest objectives. Important societal goals that might require the regulation of data flows include safeguarding personal privacy, ensuring data security, promoting fair digital competition, and — a more recent concern — establishing guardrails for the development and deployment of powerful artificial intelligence (AI) systems.

The very notion that there is a public interest in how data flows are governed is seen as a threat by data brokers; large online platforms like Google, Facebook, and Amazon; and other companies that profit from exploiting personal and non-personal data extracted from people and businesses across the world. Such data, generated when we use social media sites, shop online, search for information, use GPS systems, etc., reveal our preferences, locations, personal and work connections, health status, and more. The firms target advertising and sales and train artificial intelligence systems with our personal data and sell our information to others for various uses. To maximize the profits they generate from this business model based on the exploitation of our personal data, these firms seek to acquire, process, accumulate, store, and sell data however and wherever they choose without any oversight or limits, increasing their already oversized and problematic market power. They have branded their goal of obtaining unregulated control over our personal data as “free data flows” to suggest that any limitation on their control is a violation of our freedom.

However, policymakers around the world are increasingly discussing and adopting policies that govern the way in which data is collected, transferred, and stored, with the goal of meeting key public interest objectives. A vast majority of countries have personal data protection regimes with limits on the cross-border movement of data. In the United States and other countries, lawmakers and regulators are deploying national security measures that restrict or outright prohibit certain transactions involving sensitive data. Experts and advocates are exploring ways to adequately tax the data economy, and this could imply curbing international data transfers. Finally, the explosion of AI systems, trained on massive amounts of data, has raised questions about how to ensure that smaller companies have access to this critical resource, rather than it being monopolized by incumbent tech giants.

Expansive rules in international trade agreements that impose binding restrictions on governments’ abilities to regulate cross-border data flows and data locations run counter to these data governance efforts. Particularly, rules that effectively guarantee private corporations unfettered rights to collect, move, and store data wherever they choose would drastically undermine countries’ abilities to regulate in the digital era.

This research paper shows that such extreme restrictions have adverse implications for privacy, data security (including national security concerns), tax policy, and AI regulation. The

paper explores why and how countries are regulating data transfers in each of these areas and how nations could be affected if “digital trade” rules that privilege corporations’ imperatives over the public interest were widely adopted. The paper exemplifies the implications of such rules with a special focus on the United States, which traditionally has been a major proponent of digital rules in free trade agreements responsive to the interests of such corporations.

THE EMERGENT DATA GOVERNANCE ECOSYSTEM VERSUS THE DIGITAL TRADE RULES THAT LIMIT DATA TRANSFER AND STORAGE REGULATION

While fighting government oversight country by country, large tech firms profiting from the exploitation of data also launched a wholesale anti-regulation effort via trade agreements.[3] Powerful industries have used international trade deals to impose binding commitments on governments that favor their narrow commercial interests over the public interest. Since the early 1990s, with the launch of the World Trade Organization (WTO) and various free trade agreements, such pacts have been expanded beyond traditional trade matters like tariffs and quotas to include binding and enforceable constraints on signatory governments' domestic policies and to require that governments provide commercial entities certain rights and privileges. Countries are obligated to conform their domestic laws to trade pact rules, while the powerful enforcement systems that these deals, trade sanctions in particular, are effective in assuring compliance. And once agreed upon, the rules of such pacts cannot be modified except by the consensus of all signatory countries, thus providing a means to lock into place policies that residents of a country may oppose.

This is why certain tech interests advocate for trade agreements to include strong limits on governments' abilities to regulate international data transfers and data location. These terms — often included in "digital trade" or "e-commerce" chapters or agreements — usually ban government regulation of international data transfers[4] (cross-border data flows rules) and/or prohibit what industry calls "data localization"[5] (location of computing facilities rules). Data localization is a term used by the tech industry to describe an array of policies that require local storage of certain types of data, mandate the use of domestic servers in specified conditions, or impose other limits on where industry can process or store data. The industry has labeled the latter set of practices "data localization requirements." It is worth noting that industry lobbyists, allies, and analyses often conflate any kind of data-flow regulation with the concept of data localization in an attempt to delegitimize the mere notion of data governance.

Obviously, governments retaining the ability to regulate data flows does not mean that the transnational movement of information will stop, or that the internet will suddenly crash. Allowing countries to limit or regulate certain transfers of data merely recognizes that national governments are the entities with the power to enforce democratically adopted regulations to safeguard the public interest. The digital economy is no exception, even if the United States is just now catching up with other countries in taking action.

Indeed, it is increasingly clear that data-exploiting industry imperatives undercut protections for citizens, governments, and smaller businesses. The U.S. government is beginning to take action to address these threats. Recent U.S. policies include:

---

[3] David Dayen, "Big Tech Lobbyists Explain How They Took Over Washington," *The American Prospect*, April 18, 2023. Available from https://prospect.org/power/2023-04-18-big-tech-lobbyists-took-over-washington/.

[4] For instance, Article 19.11 of the United States-Mexico-Canada Agreement (USMCA) provides: "*No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person*."

[5] USMCA Article 19.12 bans data localization requirements in the following terms: "*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*."

- *Protecting Americans' Data from Foreign Adversaries Act of 2024*: In March 2024, the U.S. House of Representatives *unanimously* passed a bill that forbids data brokers from transferring certain types of Americans' sensitive personal information to nations deemed as foreign adversaries or entities controlled by them so as to protect American national security and individual privacy.[6] This bill was later included in a national security and foreign aid package, which was passed by both chambers of Congress and signed into law on April 24, 2024.[7]

- *Executive Order 14117 – Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*: In February 2024, the Biden administration issued an executive order to prevent access to Americans' bulk sensitive personal data and U.S. government-related data by countries of concern.[8] This policy orders the Department of Justice to issue regulations banning the acquisition, holding, use, transfer, transportation, or exportation of bulk sensitive personal data or U.S. government-related data to a foreign country of concern or a national of such a country. The Department issued its final rule in January 2025, and it became effective on April 8, 2025.[9]

- *New Cybersecurity Requirements for Cloud Computing Contractors*: In 2023, the Federal Acquisition Regulatory Council proposed a new regulation that mandates cloud computing service providers to store non-defense-related U.S. government data on servers on U.S. territory.[10] Defense-related U.S. government data has been subject to this requirement since 2015.[11]

- *Montana's Genetic Information Privacy Act*: In 2023, Montana's lawmakers passed a law that bans the storage of genetic and biometric data collected in the state in countries sanctioned in any way by the U.S. federal government.[12]

---

[6] United States, *Protecting Americans' Data from Foreign Adversaries Act of 2024*, HR 7520, 118th Congress, 2nd sess., introduced in House March 5, 2024. Available from https://www.congress.gov/bill/118th-congress/house-bill/7520/.

[7] See Division I—Protecting Americans' Data from Foreign Adversaries Act of 2024: U.S. House, *Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes*, HR 815, 118th Congress, 1st sess., introduced in House February 2, 2023. Available from https://www.congress.gov/bill/118th-congress/house-bill/815.

[8] United States, Executive Order 14117, of February 28, 2024, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern", *Code of Federal Regulations*, title 3 (2024).

[9] United States, Federal Register, *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, A Rule by the Justice Department,* January 8, 2025. Available from https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern#sectno-reference-202.301.

[10] United States, Federal Register, *Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information System, A Proposed Rule by the Defense Department, the General Services Administration, and the National Aeronautics and Space Administration,* October 3, 2023.Available from https://www.federalregister.gov/documents/2023/10/03/2023-21327/federal-acquisition-regulation-standardizing-cybersecurity-requirements-for-unclassified-federal.

[11] United States, Department of Defense, *Defense Federal Acquisition Regulation Supplement (DFARS)*, Sec. 239.7602-2 "Required Storage of Data within the United States or Outlying Areas", August 26, 2015. Available from https://www.acquisition.gov/dfars/part-239-acquisition-information-technology.

[12] State of Montana, *Genetic Information Privacy Act*, SB 351, introduced in Assembly February 15, 2023. Available from https://bills.legmt.gov/#/bill/20231/LC1085?open_tab=sum.

- *2023 Amendment to California's Confidentiality of Medical Information Act*: California legislators amended the Confidentiality of Medical Information Act to mandate in-state storage of sensitive medical information related to reproductive health and gender-affirming care, prohibiting the transfer of such information outside the state.[13]

Each of these U.S. policies fundamentally conflicts with the very notion that binding international rules should prohibit the regulation of cross-border data flows or data storage locations. As this research paper shows, the exceptions to such prohibitions that have been included in existing and proposed trade deals would not ensure governments' abilities to adopt these kinds of policies.

Former U.S. Trade Representative (USTR) Katherine Tai recognized that cementing stringent international rules about data flows and storage without first establishing U.S. domestic policies on data privacy and security would be "policy suicide."[14] She noted that Republican and Democratic members of Congress were working together to enact laws to govern data flows and establish other tech–related policies, and trade law should reflect that new reality. Notably, the most recent trade agreements negotiated by the new USTR, Jamieson Greer—such as those with Malaysia and Cambodia—do not bind the United States to allow unfettered cross-border data flows or require that the U.S. relinquish its ability to impose data-location mandates. Instead, U.S. negotiators imposed unilateral free-flow-of-data obligations only on their trading partners.[15] That divergence suggests U.S. policymakers remain wary of constraints that might undermine domestic data-governance priorities.

While U.S. policymakers grapple with this important "sequencing" problem, it is informative to consider the ways in which other countries with more established domestic privacy and data security rules in effect have shaped data-related terms in international pacts. With respect to the United States, there are only two agreements, the U.S-Mexico-Canada Agreement (USMCA) and a deal with Japan, that include the binding and expansive constraints on data regulation promoted by industry lobbyists. In contrast, other countries' agreements include terms that provide more policy space to allow public interest regulation.

The chart below compares three distinct models of international data-flow commitments. The columns, from left to right, describe the features of the 2019 USMCA; the 2021 Mercosur (*Mercado Común del Sur)* E-Commerce Agreement model; and the provisions from the 2022 European Union (EU)-New Zealand trade agreement, which represent a 2018 "horizontal" EU position on data flows agreed between the European Parliament and Commission to be included in all EU agreements.

---

[13] State of California, *Health Information*, AB 352, introduced in Assembly January 31, 2023. Available from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB352.
[14] "Fireside Chat with Katherine Tai", interviewed by David Westin, The Aspen Institute, December 7, 2023. Available from https://www.youtube.com/watch?v=nwT5GfbxTMY&t=186s.
[15] Article 3.2 of the Agreement Between the United States of America and Malaysia on Reciprocal Trade establishes: "*Malaysia shall facilitate digital trade with the United States, including by (…) ensuring the cross-border transfer of data by electronic means across trusted borders, with appropriate protections, for the conduct of business*;" Article 3.2 of the Agreement Between the United States of America and the Kingdom of Cambodia on Reciprocal Trade has an equivalent provision: "*Cambodia shall facilitate digital trade with the United States, including by refraining from measures that discriminate against U.S. digital services or U.S. products distributed digitally, ensuring the free transfer of data across trusted borders for the conduct of business, and collaborating with the United States to address cybersecurity challenges.*"

Regarding the agreements' language on data flows and location of computing facilities, there are two levels of focus: (i) the "obligations" with which countries agree to conform their domestic law; and (ii) the exceptions to those obligations, which may protect policies that would otherwise conflict with the obligations. (For a detailed analysis of the texts, please see the Appendix.)

Chart 1. Side-by-Side Comparison of Digital Trade Data-Flow Commitments in Three Key Trade Agreements

Agreement	**USMCA**	**Mercosur**	**EU-New Zealand**
Obligations			
Blanket prohibition on governments limiting data flows?	Yes	No	No
Prohibition on regulation applies broadly, not only to data moving between signatory countries?	Yes	Yes	No — limits on regulation apply to data flowing between the signatory countries only
Gives rights to companies/private parties?	Yes	Yes	No
Forbids data localization requirements?	Yes	Yes	Yes
Exceptions			
Defending countries must prove public interest policies meet a narrow trade pact necessity test and must satisfy a proportionality test that assesses their trade restrictiveness?	Yes	No	No (in the case of personal data and privacy)
Public interest policies must not arbitrarily or unjustifiably discriminate between countries?	Yes	Yes	Yes

A thorough analysis of these provisions leads to the conclusion that a potential expansion of the USMCA model would thwart data-related regulation both in the United States and abroad.

The USMCA data rules:

- establish a blanket prohibition on restrictions of cross-border movements of data, explicitly including personal data, in addition to banning data storage and processing requirements;
- apply beyond the signatory countries and forbid limitation on the movement of data to any country that a business operating in a signatory nation chooses; and
- only include a "public policy objective" exception based on the deeply flawed WTO language, which has failed to preserve countries' policy space for three decades.[16]

Both the Mercosur and the EU models have more limited commitments and allow more flexibility to regulate data transfers to meet public interest objectives. Fortunately, the USMCA language is an anomaly relative to the digital or e-commerce terms that have been included in some U.S. trade pacts since 2004. These past U.S. pacts do not include the extreme industry-favored language.

Considering this changing landscape, it is not surprising that in 2023 the U.S. government decided to withdraw its support for a 2019 proposal to include the USMCA cross-border data flows and location of computing facilities language in the E-Commerce Joint Statement Initiative (JSI).[17] The JSI is an agreement that a subset of WTO nations have been negotiating since 2017. These negotiations are arguably the most important ongoing digital trade talks, as they involve over 90 countries and, given the proponents' objective of linking them to the WTO structure and its dispute settlement system, could be enforceable with sanctions. After years of deadlock, in the summer of 2024, the proponents of this agreement announced the completion of a "stabilized text" for the first tranche of the agreement. The U.S. decision to withdraw support for the 2019 data proposals broke the JSI impasse by making clear that there was insufficient agreement among countries to include terms related to data transfers in the first tranche. Yet the new text, without data-flow obligations, that Singapore, Japan, and Australia — the countries leading the JSI talks — drafted still does not have the support of all countries participating in the negotiations. (Among the problems that the U.S. government has noted is the text's lack of an effective security exception.) Thus, a bloc of countries, including the United States, have expressed reservations over the stabilized text. The legal status of this document is uncertain.[18]

While the status of the WTO JSI on E-Commerce is uncertain, efforts to insert binding restrictions on governments' abilities to regulate cross-border data flows in international trade agreements are abound. Thus, policymakers and trade negotiators must be aware of the myriad of domestic regulatory goals that could be undermined or otherwise implicated by this

---

[16] Daniel Rangel, "WTO General Exceptions: Trade Law's Faulty Ivory Tower," Public Citizen's Global Trade Watch, last modified February 4, 2022. Available from https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/. Countries' attempts to defend their domestic policies using the language included in the public policy exception have failed in 46 of 48 attempted uses since the establishment of the WTO.
[17] David Lawder, "US Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation," Reuters, October 25, 2023. Available from https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/.
[18] Peter Ungphakorn, "Getting to Yes: What's Behind the E-Commerce Standoff at the WTO?," Hinrich Foundation, last modified August 13, 2024. Available from https://www.hinrichfoundation.com/research/wp/wto/what-is-behind-the-e-commerce-standoff-at-the-wto/.

set of rules. The rest of this research paper shows that such restrictions have adverse implications for privacy, data security (including national security concerns), tax policy, and AI regulation. Each of the following sections first explores why and how countries are regulating data transfers in each of these areas, then lays out how the United States and other nations could be affected if “digital trade” rules that privilege corporations’ imperatives over the public interest were widely adopted.

How Digital Trade Rules on Cross-Border Data Flows and the Location of Computing Facilities Can Endanger Policies Ensuring the Right to Privacy

Digital platforms and other tech firms have developed business models based on the use and sale of data, including our personal data. To maximize their profits and convenience, they seek unregulated cross-border data flows so that they can process, store, and sell data without any constraints. They have branded the concept as "free data flows" for their advocacy efforts. Although the exchange of data fosters knowledge sharing and global connectivity, there are valid grounds for regulating data collection, processing, transmission, storage locations, and retention periods, especially for certain data types.

The rise in the generation, use, and sale of large amounts of data in the digital economy has led to the pervasive practice of commercial surveillance, where every click and every search is tracked for targeted advertising and other rent-seeking practices. Information collected for such commercial purposes leads to negative spillover effects. Data-based targeting has led to most advertising revenue flowing toward dominant platforms, making it difficult for users and advertisers to switch to new competitors. In this way, dominant platforms maintain their monopolistic hold over digital markets.[19] They also take over other services, such as news media, as advertising that would otherwise have accrued to support journalism, is now gobbled up by tech giants. Excessive data collection enables some of the most problematic aspects of social media applications, which are contributing to a youth mental health crisis.[20]

As a result, many countries around the world have begun trying to protect people's rights to control their personal information through privacy legislation. But the intangibility and mobility of digital data pose regulatory challenges given the territorial nature of regulatory sovereignty and governance. Many countries have instituted restrictions or conditions on the cross-border transfer of data to try to ensure that their citizens' privacy rights are not compromised simply by moving the residents' personal data to another country.

Of the 193 countries recognized by the United Nations, 162 have passed national personal data protection laws.[21] About 75% of all countries have adopted some conditions on the cross-border transfer of data.[22] See the figure below. Only a handful of countries have no conditions or limitations on cross-border data transfers.

---

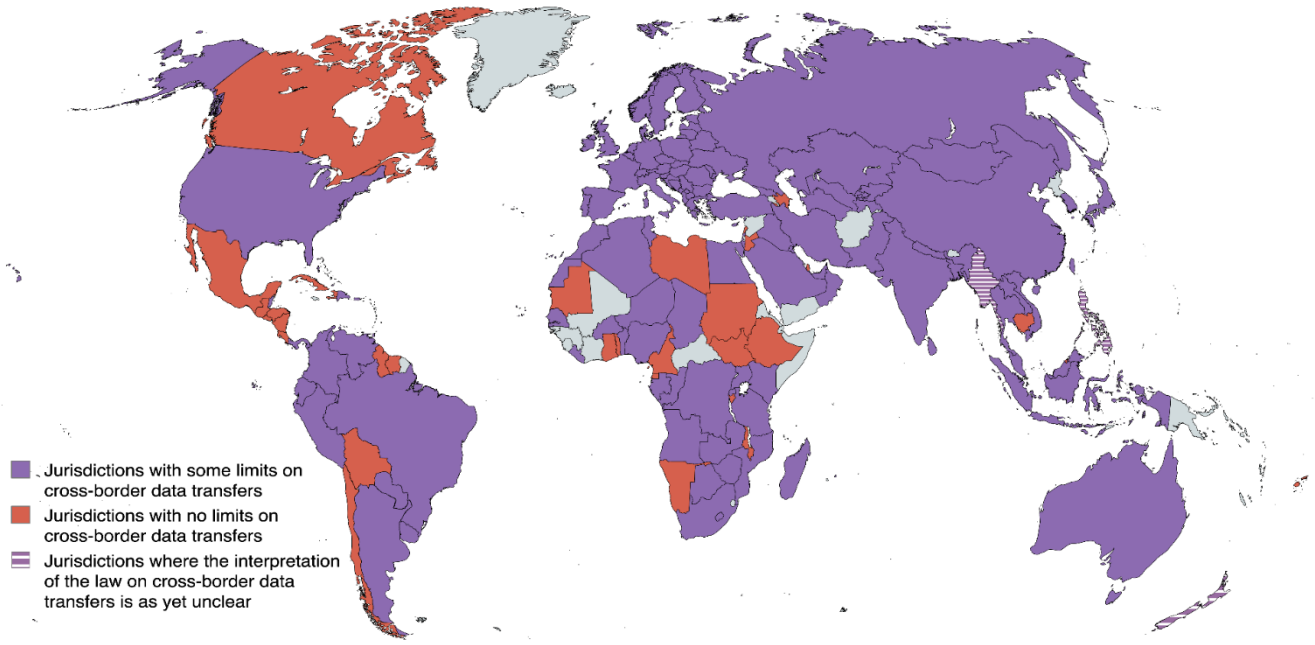
[19] U.S. House, Committee on the Judiciary, Subcommittee on Antitrust, Commercial and Administrative Law, *Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations*, 116th Congress, 2nd sess., 2020, Committee Print 117-8.

[20] World Health Organization (WHO), "Teens, screens and mental health, New WHO report indicates need for healthier online habits among adolescents", 25 September 2024. Available from https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health.

[21] Graham Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills," *181 Privacy Laws and Business International Report (PLBIR) 1, 2-4, UNSW Law Research Paper no. 23–48* (2023). Available from https://ssrn.com/abstract=4426146 or http://dx.doi.org/10.2139/ssrn.4426146.

[22] Satyajit Parekh, Stephen Reddin, Kayvaun Rowshankish, Henning Soller, and Malin Strandell-Jansson, "Localization of Data Privacy Regulations Creates Competitive Opportunities," McKinsey & Company, last modified June 30, 2022. Available from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities.

Figure 1. Countries' International Data-Transfer Policies



Source: Compiled by the authors based on data from U.S. Department of State Investment Climate Statements 2023 and DLA Piper's repository of data protection laws around the world. Created using mapchart.net. In Canada, there are specific limitations on the transfer of some kinds of data outside Québec[23] *and Ontario.*[24]

For instance, Brazil's *Lei Geral de Proteção de Dados Pessoais* (LGPD) allows for the cross-border transfer of personal data only when the receiving country has an adequate level of personal data protection, with a few exceptions.[25] Similar adequacy clauses in the United Kingdom's Data Protection Act of 2018 allow the country to choose which jurisdictions can receive personal data from UK citizens.[26] Under Kenya's Data Protection Act, transfers of personal data outside of Kenya can only take place under any one of the following circumstances: (i) the data controller or data processor can provide appropriate data protection safeguards; (ii) an adequacy decision has been made by the data commissioner; (iii) the transfer is necessary to fulfill a set of limited objectives, such as protecting the vital interests of the data subject; or (iv) the data subject has given consent.[27]

The European Union's General Data Protection Regulation (GDPR) is arguably a global high standard for personal data protection. It allows for personal data transfer only to jurisdictions

[23] Candice Hévin and Simon Du Perron, "Cross-Border Transfers of Personal Information Outside Québec: Requirements for Businesses," Borden Ladner Gervais LLP, last modified May 7, 2024. Available from https://www.blg.com/en/insights/2022/12/cross-border-transfers-of-personal-information-outside-quebec.
[24] Candice Teitlebaum and Aaron Collins, "Canadian Privacy Legislation and the Cross-Border Transfer of Personal Information Part One: Personal Health Information," Aird & Berlis LLP, last modified May 2008. Available from https://www.airdberlis.com/docs/default-source/articles/article---cross-border-transfer-of-personal-health-information.pdf?sfvrsn=2.
[25] Brazil, *Lei Geral de Proteção de Dados Pessoais (LGPD)*, Article 33 I of Law No. 13.709 (2018). Available from https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.
[26] United Kingdom, *Data Protection Act 2018*, Sections 73 and 74, UK Public General Acts (2018). Available from https://www.legislation.gov.uk/ukpga/2018/12/section/73/enacted.
[27] Kenya, *The Data Protection (General) Regulations,* Kenya Gazette Supplement, Part VII, No. 236 (2021). Available from https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf.

with a certain level of data protection.[28] The European Commission makes these decisions on the basis of an "adequacy" determination, which provides that the countries where the data can be freely transferred have a level of privacy protection equivalent to that of the EU. If no such adequacy determination is made, data can be transferred outside the EU under binding corporate rules for intra-company transfers or standard contractual clauses for inter-company transfers. The liability for breaches, however, remains with the EU entity carrying out the transfer.[29] In practice, companies widely use such standard contractual clauses to transfer data out of the EU.[30]

As of 2025, the European Commission has recognized Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States (only for commercial organizations participating in the EU-U.S. Data Privacy Framework[31]), and Uruguay as providing adequate protection such that data can flow freely between the EU and these jurisdictions without additional safeguards.[32]

Box 1: The EU's Model to Safeguard Privacy From Trade Pact Obligations

Privacy is considered a basic human right in the European Union. Before the GDPR, data-related privacy rights in the EU were governed by the 1995 Data Protection Directive.[33] It established conditions for lawful data processing, individuals' personal data protection rights, and principles of data quality. In 2009, the European Commission reviewed this directive in light of the increased use by economic actors and public authorities of digital data as well as, interestingly, the spread of cloud computing.[34] The European Commission deemed that cloud computing (computing over remote servers) might involve "the loss of individuals' control over their potentially sensitive information when they store their data with programs hosted on someone else's hardware."[35] Underlying the review was an assumption by the European

[28] European Union, *General Data Protection Regulation (GDPR)*, Article 45(3), Official Journal of the European Union (2016). Available from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[29] European Union, GDPR, Article 47.2(f); *Commission Implementing Decision (EU) 2021/914: On Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, Clause 12(b), Official Journal of the European Union (2021). Available from https://publications.europa.eu/resource/cellar/55862dbf-c72b-11eb-a925-01aa75ed71a1.0006.01/DOC_1.
[30] Svetlana Yakovleva and Kristina Irion, "Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation," *American Journal of International Law,* vol. 114, no. 10 (2020), pp. 10–14. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524245.
[31] The adequacy finding for the United States is premised on self-certification systems and the Biden Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities. The European Court of Justice invalidated previous U.S. adequacy findings and has not yet ruled on the latest version.
[32] European Commission, "Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection," accessed October 28, 2024. Available from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[33] European Union, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data," Official Journal of the European Union (1995). Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.
[34] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, European Commission (2010). Available from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.
[35] *Communication from the Commission: A Comprehensive Approach on Personal Data Protection*.

Commission that personal data protections for EU citizens should not change depending on where their data happens to be stored or processed. The Commission decided then to examine how citizens could be granted the same degree of protection as was required within the EU when their data was stored in a third country.[36]

Under the Data Protection Directive, other countries' policies and practices were assessed to determine if they provided *adequate* privacy protection. Based on these rules, the European Commission issued both the Safe Harbor decision in 2000 and the EU-U.S. Privacy Shield in 2016, which allowed the transfer of European personal data to certain U.S.-based companies. Both of these determinations were struck down by the Court of Justice of the European Union on the grounds that U.S. surveillance laws do not limit personal data requests to what is strictly necessary and proportionate. At the same time, the Commission became concerned about the lack of clear criteria in the Directive to guide adequacy decisions, as well as the fact that — under the Directive — both the Commission and individual Member States could grant adequacy decisions, which could lead to conflicting outcomes.[37]

The 2009 review resulted in proposed changes to the adequacy regime for international data transfers, including a new requirement to review the third country's legal system based on a clear set of parameters. Basically, the Commission proposed that in order to grant an adequacy decision, it would have to review the following aspects of the third country's legal system: (i) public security, defense, national security and criminal laws with regard to access of public authorities to personal data; (ii) whether the jurisdiction grants effective and enforceable individual rights and effective administrative and judicial redress; and (iii) the existence and effective functioning of one or more independent supervisory authorities in the foreign jurisdiction. These changes were ultimately included in the 2016 GDPR as the successor to the Directive's EU policy on data privacy.[38] It quickly became clear that there was a tension between the inclinations of the European Commission division negotiating trade agreements, the Directorate-General for Trade, or "DG Trade," which was supportive of the industry demand for unrestricted cross-border data flows, versus the privacy-first GDPR.[39] In particular, a 2016 study by professors Kristina Irion, Svetlana Yakovleva, and Marija Bartl clarified that the applicable WTO general exceptions language, which is replicated in many other trade pacts, would not protect the GDPR and the privacy rights it provided from conflicting with the expansive "data free flows" commitments being contemplated in various trade negotiations.[40] This study triggered an EU-wide debate over trade and privacy, with the European Parliament being intensively involved in the development of a new approach. In 2018, the European Commission adopted a new position often referred to as the "EU's horizontal provisions on cross-border data flows and personal data protection." It is the basis for the EU's 2019 proposed text on data flows and storage at the JSI negotiations.[41]

---

[36] *Communication from the Commission: A Comprehensive Approach on Personal Data Protection*.
[37] *Communication from the Commission: A Comprehensive Approach on Personal Data Protection*, p. 15.
[38] Article 45(2)(a) and (b) of the EU's General Data Protection Regulation.
[39] Svetlana Yakovleva and Kristina Irion, "Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade," *International Data Privacy Law* vol. 10, no. 3 (2020), pp. 201–221. Available from https://doi.org/10.1093/idpl/ipaa003.
[40] Kristina Irion, Svetlana Yakovleva and Marija Bartl, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements*, Institute for Information Law, University of Amsterdam (2016). Available from https://dare.uva.nl/search?identifier=2a4a80a7-fcb3-4ee9-8b01-11a2e2cdf17a.
[41] World Trade Organization, "Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce," INF/ECOM/22, April 26, 2019. Available from https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/22.pdf&Open=True.

This approach includes language like that found in the 2012 U.S.-Korea Free Trade Agreement, which calls on parties to enable cross-border data transfers but does not include the USMCA language banning restrictions on transfers.[42] However, the EU horizontal provisions also include binding language that explicitly forbids specific enumerated forms of data localization requirements. This includes bans on, among others, requiring the use of computing facilities or network elements in the signatory's territory for data processing or requiring the localization of data in the signatory's territory (see Appendix for exact language). GDPR does not require the localization of EU residents' data in the EU; instead, it regulates the conditions under which data can be transferred to non-EU countries. This means that, in principle, the ban on data localization practices should not compromise the GDPR. However, to create ironclad protections for GDPR's data privacy guarantees and to safeguard policy space for any other future privacy policy that may employ different mechanisms, the horizontal provisions also include an effective exception for personal data protection and privacy policies: "*Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.*"[43]

The first pact to fully include this model was the EU-New Zealand free trade agreement (FTA), signed in 2022. Before, in 2021, the EU and the UK signed their post-Brexit trade and cooperation agreement, but this deal departed slightly from the horizontal provisions in terms of the exception language.[44] The EU-New Zealand agreement, however, includes the full privacy exception as drafted in the horizontal provisions.[45] It also provided for a review of this section in three years with a commitment from the New Zealand government to include Māori in the review process.[46]

In 2022, the EU and Japan decided to start negotiations on data transfers in the context of their Economic Partnership Agreement.[47] In 2023, a deal was announced.[48] The new text departs in important ways from the EU horizontal provisions and can be perceived as a backsliding with respect to deals the EU had negotiated both with the UK and New Zealand. First, the EU-Japan deal includes more prohibitions than those proposed by the horizontal provisions, such as a ban on requiring the approval of a government entity prior to the transfer of information to the territory of the other party. Moreover, the new text adds conditions that a government would have to meet in order to avail itself of the privacy exception. Specifically, to

[42] Joint Statement on E-Commerce: EU Proposal, Sec. 2.7.1.
[43] European Commission, "Horizontal Provisions on Cross-Border Data Flows and Personal Data Protection", last modified May 18, 2018. Available from https://ec.europa.eu/newsroom/just/items/627665.
[44] European Commission, "EU-UK Trade and Cooperation Agreement," conclusion date: December 30, 2020, Art. 202. Available from https://commission.europa.eu/strategy-and-policy/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en.
[45] European Commission, "Free Trade Agreement Between the European Union and New Zealand," conclusion date: July 9, 2023, Ch. 12, Sec. B, Art. 12.5. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400229#page=99.
[46] "FTA Between the EU and New Zealand," Ch. 12, Sec. B, Article 12.4.
[47] European Commission, "Landmark EU-Japan Data Deal One Step Closer to Ratification," last modified December 1, 2023. Available from https://policy.trade.ec.europa.eu/news/landmark-eu-japan-data-deal-one-step-closer-ratification-2023-12-01_en.
[48] European Commission, "EU and Japan Conclude Landmark Deal on Cross-Border Data Flows at High-Level Economic Dialogue," last modified October 27, 2023. Available from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378.

qualify for the exception, a privacy policy must enable international data transfers under conditions of general application, which must be formulated in objective terms. The immediate consequences of these terms might not seem especially problematic given that the EU has deemed that Japan has an adequate level of data protection, creating a de facto system of unrestricted personal data transfers in any case.[49] However, if the EU eventually decided to revoke the adequacy determination for Japan due to changes in Japan's data protection regime or stricter GDPR enforcement particularly regarding onward data transfers to third countries,[50] Japan could successfully challenge such a decision based on the new data-transfer deal.

Many of the governments that retain policy space for domestic storage requirements for some kinds of data do not, as a rule, advocate for extensive data localization. For instance, the African Union's Data Policy Framework of 2022 discourages data localization but recognizes that very specific localization requirements for some sensitive categories of data agreed upon through multi-stakeholder consultations can be instituted. It also recommends that such measures be evaluated for potential harm to human rights.[51]

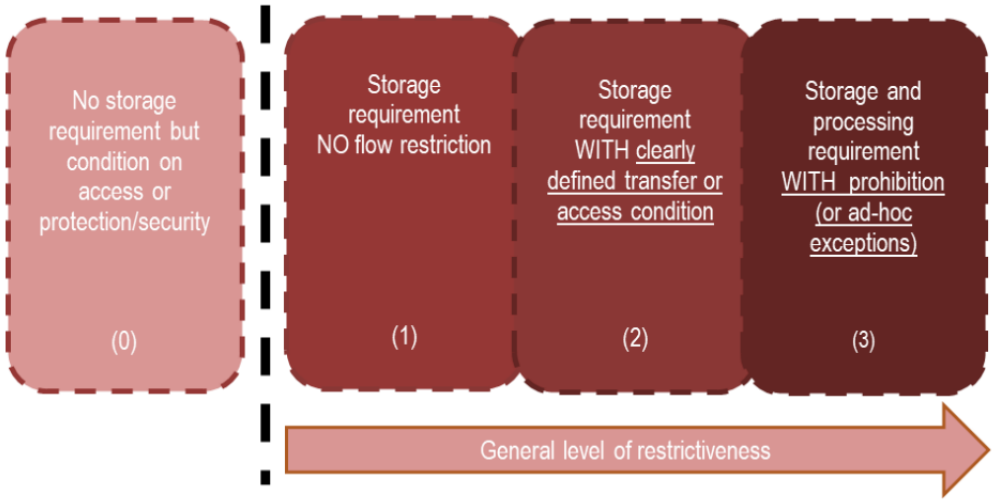
The tech industry's claims of alleged rising barriers to cross-border data flows are disingenuous. Given that the regulation of international data transfers is a relatively new policy concern, countries, naturally, are just now starting to adopt policies in this domain. Compared with mature industries such as heavy metals manufacturing, the number of alleged "barriers to trade" are still very low. For instance, in 2021, the Information Technology and Innovation Foundation, a Big Tech-funded think tank, sounded the alarms because it identified 144 "data flows restrictions" adopted by 62 countries worldwide.[52] This number pales in comparison with alleged trade restrictions adopted in traditional sectors. For instance, between 2009 and 2021, the University of Saint Gallen's Global Trade Alert database on trade policy interventions documented 769 potentially trade-restrictive measures adopted by countries concerning solely iron and steel products.[53] Yet iron and steel exports worldwide reached $586 billion in 2021, increasing by $170 billion compared to 2017.[54] This clearly indicates that policies perceived as "trade barriers" might affect international exchanges but by no means halt trade flows.

Moreover, governments that have adopted domestic storage requirements have chosen to calibrate the strictness of their policies depending on their desired level of protection. An

[49] European Commission, "European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows," last modified January 22, 2019. Available from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.
[50] See Svetlana Yakovleva, "Scope and Applicability of Free Data Flow Exceptions in US-Japan Digital Trade Agreement and the CPTPP", Digital Trade Alliance *Japan's 'Data Free Flow with Trust' Versus Digital Trade Agreement Commitments* series (2023). Available from https://dtalliance.org/wp-content/uploads/2023/02/Scope-and-Applicability-of-Free-Data-Flow-Exceptions-in-US-Japan-Digital-Trade-Agreement-and-the-CPTPP.pdf.
[51] Mercy King'Ori, Ulric Quee, and Hunter Dorwart, "The African Union's Data Policy Framework: Context, Key Takeaways, and Implications for Data Protection on the Continent", Future of Privacy Forum, last modified March 29, 2023. Available from https://fpf.org/blog/the-african-unions-data-policy-framework-context-key-takeaways-and-implications-for-data-protection-on-the-continent/.
[52] Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", Information Technology and Innovation Foundation, last modified July 1, 2021. Available from https://www2.itif.org/2021-data-localization.pdf.
[53] "Global Dynamics," Global Trade Alert, accessed November 21, 2024.
[54] World Trade Organization, *World Trade Statistical Review 2022*. Available from https://www.wto.org/english/res_e/booksp_e/wtsr_2022_e.pdf.

Organisation for Economic Co-operation and Development (OECD) report shows that countries' restrictions on cross-border data transfers fall on a spectrum.[55] Sometimes, governments require only that a copy of the data be stored locally so as to make it available for government inspection, with no restriction on other copies being stored in foreign data centers. Sweden's Accounting Act is an example of this.[56] Some laws require that a copy be stored locally and that other copies be stored only in jurisdictions considered appropriate or safe — for instance, Australia's Electronic Health Records Act.[57] Other laws require that certain categories of data be stored only domestically — for instance, India's insurance law requires that all insurance data be stored in domestic data centers only.[58]

Figure 2. OECD Typology of Data Localization Measures and Requirements for Data Flows



Note: Figure is schematic; elements do not singularly identify any given country's approach to data localisation. Different approaches tend to apply to different types of data, even within a same jurisdiction.

Source: OECD.[59]

Other countries have tried to promote voluntary systems for conditions on cross-border data transfers. For instance, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System (CBPR) is an opt-in privacy code of conduct for companies located in APEC member countries.[60] In 2022, the U.S. Department of Commerce announced that this system would evolve into a "Global CBPR Forum" open to other countries, but it remains unclear whether the initiative will gain traction.[61] Under CBPR, participating countries have to demonstrate that privacy rules meeting the CBPR's standards are legally enforceable in their own jurisdictions. However, these standards are relatively weak. For example, they require data collectors to limit data collection to specific purposes and to inform individuals when their

[55] Javier López González, Francesca Casalini, and Juan Porras, "A Preliminary Mapping of Data Localisation Measures," OECD Trade Policy Papers, no. 262 (2022). Available from https://doi.org/10.1787/c5ca3fed-en.
[56] González, Casalini, and Porras, "A Preliminary Mapping."
[57] González, Casalini, and Porras, "A Preliminary Mapping."
[58] India, *IRDAI (Maintenance of Insurance Records) Regulations*, Paragraph 3(9), The Gazette of India (2015). Available from https://irdai.gov.in/document-detail?documentId=604674.
[59] González, Casalini, and Porras, "A Preliminary Mapping."
[60] "The APEC Cross-Border Privacy Rules (CBPR) System," Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, accessed March 21, 2024. Available from https://cbprs.org/.
[61] Graham Greenleaf, "Global CBPRs: A recipe for failure?," University of New South Wales Law & Justice Research Series, 177 *Privacy Laws & Business International Report* 11–13 (2022). Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4180516.

data is being collected.[62] Unlike stricter data protection regimes, companies are not required to minimize data collection nor prohibited from transferring specific types of sensitive information to third parties. Under this framework, companies can be certified as CBPR-compliant by third-party private firms, called accountability agents, by demonstrating that they meet the CBPR privacy standard. The CBPR does not institute binding and comprehensive conditions on cross-border data transfers. Unlike the GDPR, the conceptual basis of the CBPR is not protection of human rights but rather protection against individual risk or harm, like in tort law.[63] The CBPR does not protect personal data that is not directly collected from data subjects, and its purpose limitations are very broad.[64] Other protections in the CBPR are similarly diluted in comparison to the GDPR.[65] In fact, all countries approved to participate in the CBPR (except the United States) already have stronger data privacy laws than the APEC CBPR regime. Given the CBPR's relatively low standards compared to the domestic privacy laws of most countries, the system has largely failed to meet its goal of facilitating data transfers among participating economies.[66] These aspects make the CBPR an uncertain and generally weak data protection framework.

Acknowledging the weakness of voluntary schemes such as CBPR is relevant because under most cross-border data movement and location of computer facilities "digital trade" rules, even flexible conditions on data transfers or soft local storage requirements could be deemed inconsistent with trade pact commitments. Indeed, under the USMCA model described above, any kind of restriction on the movement of data across borders would be a violation of the cross-border data-flow rule. This includes privacy regimes like GDPR or similar laws adopted by dozens of countries worldwide. Moreover, even a flexible policy like Sweden's Accounting Act, which requires a copy of accounting data be stored locally without restricting the possibility of other copies being stored in foreign data centers, would be a data localization requirement banned by most "digital trade" rules on data storage. The expansive nature of these prohibitions and, as explained in the box below, the way in which the balance between data protection and unhindered movement of data in most existing digital trade agreements is skewed toward the latter means that countries could be forced to adopt less protective domestic privacy regimes if they want to comply with "digital trade" rules.

Box 2: So-called "public policy" exceptions based on the WTO's GATT/GATS general exception undermine countries' capacities to choose their desired level of data protection

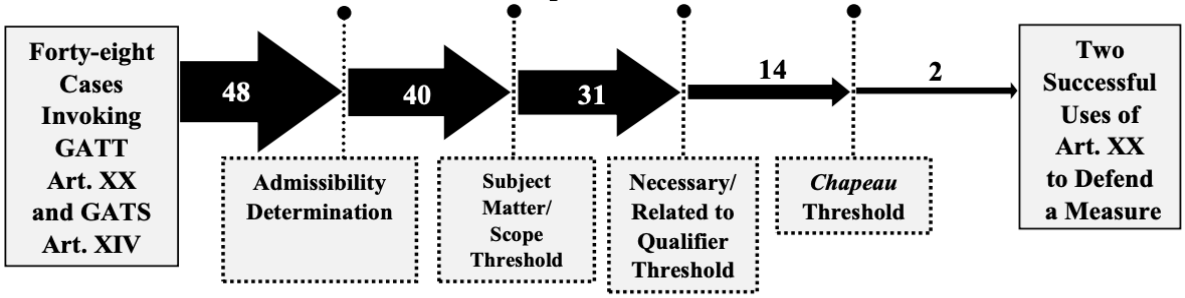
The USMCA model for rules on "cross-border data flows" imposes strict constraints on governments' rights to regulate data flows with a specific exception based on the WTO General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in

[62] "Template Notice of Intent to Participate in the APEC Cross Border Privacy Rules System," Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, last modified November 2019. Available from https://cbprs.org/wp-content/uploads/2019/11/6.-Template-Notice-of-Intent-to-Participate-in-the-CBPR-System-updated-17-09-2019.pdf.
[63] Clare Sullivan, "EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era", *Computer Law & Security Review,* vol. 35, no. 4 (2019), pp. 380–397. Available from https://doi.org/10.1016/j.clsr.2019.05.004.
[64] Sullivan, "EU GDPR or APEC CBPR?"
[65] Sullivan, "EU GDPR or APEC CBPR?"
[66] Greenleaf, "Global CBPRs: A recipe for failure?"

Services (GATS) general exceptions. Over the years, scores of trade tribunal rulings have proven these exceptions to be largely ineffective. Tribunals have ruled against the use of GATT and GATS general exceptions to defend countries' domestic policies in 46 of 48 attempts since the WTO started in 1995.[67]

One of the main issues with the WTO model for exceptions language is the use of proportionality tests to assess the trade restrictiveness of a policy. Some WTO exceptions only allow countries to justify public interest policies under the exceptions when they are "necessary" to meet their public interest goal. This means that if policymakers or regulators opt for policies that a trade tribunal concludes are "more restrictive than necessary," the policies cannot be justified under the exceptions. This requirement was incorporated in USMCA's terms on cross-border data flows and a number of other agreements (see Appendix for the specific language).

Figure 1. The Pathway for the Two Instances of Respondents Successfully Invoking the General Exceptions Defense



Source: Public Citizen.[68]

In the context of data policies, for instance, if a country chooses to require that copies of sensitive health data are stored locally and that copies of such data are only stored in jurisdictions considered appropriate or safe, like Australia does, another country could claim that this limitation on the cross-border movement of data is more restrictive than necessary. The challenging country could argue that Australia should rely on less restrictive policies, like only requiring that a copy of health data is stored locally without regulating whether other copies are stored abroad or trusting companies' compliance with the weak APEC CBPR framework. If a trade tribunal agrees with that argument — and, as the chart above shows, many attempted uses of the exception language have failed on this very test — Australia's policy would not be safeguarded by the exception and would be deemed inconsistent with the trade agreement. A ruling against such data policy could expose the regulating country to millions in retaliatory tariffs that stay in place until the policy is changed, which in turn could put pressure on policymakers and regulators to roll back or weaken the policy.

[67] Daniel Rangel, *WTO General Exceptions: Trade Law's Faulty Ivory Tower*, Public Citizen's Global Trade Watch, last modified February 4, 2022, pp. 18–19. Available from https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_-1.pdf.
[68] Rangel, *WTO General Exceptions*.

DIGITAL TRADE RULES DO NOT SAFEGUARD DATA SECURITY POLICIES

The security of sensitive data and algorithms is another consideration that drives international data transfer regulation and domestic data storage requirements in many countries. Data security implicates people's personal security, as well as the economic security of individuals and businesses. In the United States in recent years, the data security debate has focused significantly on national security, which has also been the focus of some other countries' data security policies. South Korea demonstrates an interesting use case. South Korea's Land Survey Act prevents the unrestricted transfer of map data outside the country due to national security concerns. The government has offered to allow cross-border map data transfers, but only with the locations of sensitive infrastructure blurred out.[69]

At the EU level, a discussion on data sovereignty is taking place surrounding the European Cybersecurity Certification Scheme for Cloud Services (EUCS), proposed by the European Union Agency for Cyber Security (ENISA) in 2020 based on the EU Cybersecurity Act. Data sovereignty requirements were included in subsequent drafts after pressure from several member states, primarily France. These drafts required companies offering certain types of services with a need for the highest security standards to be immune from foreign law and process data solely within the EU. The certification scheme is still being heavily discussed. Although certification is voluntary based on the Cybersecurity Act, they could legally be made mandatory under an EU-wide cybersecurity instrument called the NIS2 Directive for certain entities by the European Commission or member states. Governments could also require such a certification in public procurement, making them de facto mandatory.[70]

The United States, too, has instituted domestic data storage requirements for sensitive defense-related data. Since 2015, the Defense Federal Acquisition Regulation Supplement requires cloud computing service providers to maintain all defense-related government data that is not physically located on the Department of Defense premises within U.S. territory, unless otherwise authorized by the authorizing official.[71] In October 2023, the Department of Defense, General Services Administration, and the National Aeronautics and Space Administration (NASA) proposed expanding this requirement to non-defense, high-impact federal information systems by amending the Federal Acquisition Regulation (FAR). This proposal — based on an executive order requiring agencies to standardize cybersecurity contractual requirements — is going through the rulemaking process.[72] The policy is flexible; it allows for cross-border data transfer with the approval of a relevant authorizing official.[73] However, even such a flexible policy linked to legitimate national security interests would run the risk of violating the extreme language forbidding government regulation of data.

---

[69] Julia Yoon, "South Korean Data Localization: Shaped by Conflict," University of Washington, Henry M. Jackson School of International Studies, last modified February 28, 2018. Available from https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/.
[70] Lisa Peets, Marty Hansen, Mark Young, and Bart Szewczyk, "Implications of the EU Cybersecurity Scheme for Cloud Services," Inside Privacy, November 1, 2023. Available from https://www.insideprivacy.com/cybersecurity-2/implications-of-the-eu-cybersecurity-scheme-for-cloud-services/.
[71] U.S. Department of Defense, *DFARS*, Section 239.7602-2.
[72] United States, Federal Register, *Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information System*.
[73] U.S. Department of Defense, *DFARS*, Section 239.7602-2.

Perhaps most importantly, these broad restrictions on data regulation, if agreed on at a plurilateral level, would prohibit the new restrictions on data brokers established by the U.S. Congress in the Protecting Americans' Data from Foreign Adversaries Act of 2024. On April 24, 2024, President Biden signed into law a national security and foreign aid package which included the Protecting Americans' Data from Foreign Adversaries Act of 2024. This law, which the U.S. House of Representatives unanimously passed, prohibits data brokers from transferring U.S. residents' sensitive data to foreign adversaries.[74] The law explicitly forbids certain data transfers, which would violate the JSI cross-border data flows terms proposed by the U.S. government in 2019, from which support was withdrawn in 2023 consistent with new domestic policy.

The proposed constraints would also undermine President Biden's February 28, 2024, executive order on data security and its implementing regulation, which became effective on April 8, 2025. That order called for the Department of Justice to issue regulations to prohibit the transfer of bulk sensitive personal data and U.S. government data to countries of concern.[75] In January 2025, the Department of Justice issued its final rule implementing the order.[76] According to the new regulation, certain classes of highly sensitive transactions with countries of concern or entities linked to these countries are prohibited. This includes, for instance, data brokerage arrangements that give access to bulk sensitive personal data, including personal identifiers, precise geolocation data, biometrics, health data, and financial data. Some other transactions are restricted, unless they comply with predefined security to mitigate the risk of access to bulk U.S. sensitive personal data by malign actors. While this policy does not establish "generalized data localization requirements," trade pact rules — particularly in the context of the WTO — that could ban *all* conditions on cross-border data transfers would expose it to challenges at a trade agreement enforcement tribunal.

It is important to note that while the version of the JSI text most recently proposed by the countries leading those talks does not include terms regarding data transfers, it does include exceptions that would apply to the entire deal.[77] The text merely states that the corresponding security exceptions of the WTO GATT and GATS apply to this agreement. But the GATT and GATS security exceptions set forth limited grounds for when a country may be able to justify policies otherwise inconsistent with the rules. Basically, the exceptions can only potentially defend security policies related to fissionable materials or military supplies trade, or in cases of war or "other emergency in international relations."

Countries have limited abilities to successfully use the WTO security exceptions to defend domestic policies, given that WTO enforcement tribunals have interpreted the concept of "emergency in international relations" very narrowly. Indeed, WTO panels ruled against the United States on two occasions already with respect to U.S. attempts to use this security

---

[74] Angelika Munger, "House Passed New Bill to Prohibit Data Brokers from Transferring Sensitive Data to Foreign Adversaries," *The National Law Review*, March 21, 2024. Available from https://www.natlawreview.com/article/house-passed-new-bill-prohibit-data-brokers-transfering-sensitive-data-foreign.

[75] Executive Order 14117.

[76] United States, Federal Register, *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, A Rule by the Justice Department,* January 8, 2025. Available from https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern#sectno-reference-202.301.

[77] World Trade Organization, "Joint Statement Initiative on Electronic Commerce," INF/ECOM/87, July 26, 2024. Available from https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True.

exception to defend various China-related trade policies.[78] These rulings made clear that the GATT/GATS security exception model is completely ineffective in a world of increasing geopolitical tensions. Namely, trade tribunals seem to have concluded that a country must be engaged in active military conflict with another nation or on the brink thereof to meet the "emergency in international relations" condition.

The security exception that the United States has included in its FTAs since the pact signed with Singapore in 2003 provides an example of a more effective approach, which could be applied to rules governing the regulation of data transfers. The U.S. FTA security exception language basically ensures that each country determines its essential security interests and whether the policies it adopts are necessary to protect such interests.[79] More recent U.S. agreements, such as those with Peru or Korea, even include a footnote stating that the tribunal or panel adjudicating such a complaint shall find that the exception applies if the security exception is invoked in the dispute settlement procedure of the FTA. The digital trade rules in the Regional Comprehensive Economic Partnership, an initiative led by the Association of Southeast Asian Nations (ASEAN), include such a self-judging security exception, which allows countries to determine the content of their essential security interests. As with the U.S. FTA security exception language in recent agreements, a country's self-assessment of its security interests is not open to challenge by other countries.[80]

If trade agreements contain rules on cross-border data transfers, given that countries will regulate data issues for national security purposes, such pacts will require self-judging security exemptions such that countries retain sovereignty over data-related security decisions. Yet the absolute need for such an expansive security exception raises a key question: Is it really wise to commit to unfettered data transfers, particularly among geopolitical rivals, in a world where security-related regulation in the digital sphere grows more and more important every day?

[78] World Trade Organization, "United States – Certain Measures on Steel and Aluminium Products: Report of the Panel," WT/DS544/R, December 9, 2022. Available from https://www.worldtradelaw.net/document.php?id=reports/wtopanels/us-steelaluminum(panel)(china).pdf; World Trade Organization, "United States – Origin Marking Requirement: Report of the Panel," WT/DS597/R, December 21, 2022. Available from https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/597R.pdf&Open=True.
[79] U.S.-Singapore Free Trade Agreement, conclusion date: May 6, 2003, Art. 21.2(b). Available from https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf#page=233.
[80] Regional Comprehensive Economic Partnership (RCEP), conclusion date: November 15, 2020, Art. 12.14(3)(b). Available from http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_en.pdf#page=9.

DIGITAL TRADE INTRUSIONS IN GOVERNMENTS' ABILITIES TO GOVERN DATA TRANSFERS COULD AFFECT TAX POLICY

As Big Tech corporations continue to dominate the global economy, these firms' monopoly power has led to concerns about adequate taxation. The digitalization of the economy leads to two interconnected taxation problems:

> **Base erosion and profit shifting**: The dominance of multinational companies can erode local tax bases. This issue is pervasive across economic sectors, but the damage is especially acute when it comes to digital services that can be delivered from anywhere in the world. When governments seek to tax profit, companies can report profit in low-tax jurisdictions to minimize the taxes they pay globally. The OECD estimates that, globally, $240 billion is lost annually due to tax avoidance by multinational companies.[81]
>
> **Taxation of intangibles and the use of data**: Value drivers in the digital economy can often be intangible and do not require a physical presence in most jurisdictions where digital companies operate. Data is, of course, a key input of the value generated by digital companies (explaining much of their advocacy for unrestricted cross-border data flows). Traditional tax systems are unable to appropriately tax economic activities with these characteristics. Moreover, many scholars, governments, and international organizations now view data as an economic resource and believe that some of its value belongs to the populations from which it is being generated. [82]

To overcome these challenges, experts and policymakers have considered a number of proposals for taxing the collection or sale of certain data, including in the United States. In Washington state in 2017, for instance, State Rep. Norma Smith proposed HB 1904, which would impose a business and occupation tax of 3.3% on the sale of personal data related to residents of Washington state.[83] Washington's House Committee on Technology and Economic Development recommended passage of the bill in 2017. However, after industry lobbyists testified against it,[84] the proposal was not adopted by the full legislature.[85] There

---

[81] "Base Erosion and Profit Shifting (BEPS)," Organisation for Economic Co-operation and Development, accessed November 1, 2024. Available from https://www.oecd.org/tax/beps/.

[82] Satyanarayana Jeedigunta, Purushottam Kaushik, Nadia Hewett, and Arushi Goel, "Towards a Data Economy: An Enabling Framework," World Economic Forum White Paper (2021). Available from https://www.weforum.org/publications/towards-a-data-economy-an-enabling-framework/; Stuart Mills, "Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership," SSRN Working Paper (2019). Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3437936; "Capitalizing on the Data Economy," MIT Technology Review Insights, last modified November 16, 2021. Available from https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/.

[83] Washington State Legislature, *Relating to the Sale and Taxation of Washingtonians' Personal Information and Related Data*, HB 1904, introduced in House February 2, 2017. Available from https://apps.leg.wa.gov/billsummary/?BillNumber=1904&Year=2017&Initiative=false.

[84] John Stang, "Proposed State Tax on Sale of Personal Data Faces a Fight from Business Groups," GeekWire, March 11, 2017. Available from https://www.geekwire.com/2017/proposed-state-tax-sale-personal-data-faces-fight-business-groups/.

[85] Omri Marian, "Taxing Data," *BYU Law Review,* vol. 47, no. 2 (2022). Available from https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=3349&context=lawreview; Washington State Legislature, HB 1904.

have been multiple data taxation proposals in New York since at least 2019.[86] A similar "data dividend" proposal has been made by California Governor Gavin Newsom.[87]

Policies taxing the sale, transfer, or processing of data could be challenged under the most invasive trade agreement formulations banning international data-transfer regulation. As mentioned before, the USMCA model for cross-border data flows obligations bans any kind of prohibition or *restriction* on the international movement of data. It is important to note that the term "restriction" has been broadly interpreted by trade law international adjudicating bodies. For instance, the WTO Appellate Body defined *restriction* as "*'[a] thing which restricts someone or something, a limitation on action, a limiting condition or regulation', and thus refers generally to something that has a limiting effect.*"[88] The broad interpretation of restrictions under international trade law means that the USMCA obligation to preserve free data transfers could encompass a wide range of policies that might merely affect or condition — but not necessarily ban — the movement of data across borders.

For instance, if Washington state enacted a tax on the sale of personal data and this tax discouraged some firms from selling data to overseas customers, a business or a group of businesses located in a USMCA country could claim that the personal data sales tax is an illegal restriction on the cross-border movement of data. If said business or group of businesses successfully recruited their government to launch a dispute against this policy, it would be hard to argue that a sales tax that could indeed reduce the number of data transfers — and in a way might be intended to do exactly that — is not a restriction on the movement of data. This means that the United States would have to rely on the deficient exception language included in the USMCA (see Box 2) to try to defend this policy from a trade challenge; if lost, the challenge could result in trade sanctions until the policy was eliminated.

Such conflicts with prospective measures that, even if not yet adopted, could be part of future data governance frameworks highlight the dangers of adopting broad obligations limiting the regulation of international data transfers.

---

[86] New York State Senate, *Creates an Excise Tax on the Collection of Consumer Data by Commercial Data Collectors*, SB 4959, introduced in Senate February 19, 2021. Available from https://www.nysenate.gov/legislation/bills/2021/S4959; New York State Senate, *Establishes the Office of Consumer Data Protection and Imposes a Tax on Data Controllers and Data Processors*, SB 6727, introduced in Senate May 13, 2021. Available from https://www.nysenate.gov/legislation/bills/2021/S6727; New York Senate, *Relates to a Tax on Gross Income Upon Every Corporation which Derives Income from the Data Individuals of this State Share with Such Corporations*, SB 6102, introduced in Senate May 16, 2019. Available from https://www.nysenate.gov/legislation/bills/2019/S6102.

[87] Jasmine Ulloa, "Newsom Wants Companies Collecting Personal Data to Share the Wealth with Californians," *Los Angeles Times*, May 5, 2019. Available from https://www.latimes.com/politics/la-pol-ca-gavin-newsom-california-data-dividend-20190505-story.html.

[88] World Trade Organization, "China – Measures Related to the Exportation of Various Raw Materials: Reports of the Appellate Body," WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, January 30, 2012, para. 319. Available from https://www.wto.org/english/tratop_e/dispu_e/394_395_398abr_e.pdf.

LIMITS ON THE REGULATION OF DATA MOVEMENT COULD UNDERMINE AI POLICY AND DATA REGULATION BEYOND PERSONAL DATA PROTECTION

The explosive growth in AI technology in recent years has brought back into focus the importance of personal *and non-personal data* as a resource. While traditionally personal data protection has been the focus of regulation, recently, policymakers have started to take an interest in non-personal data. Non-personal data is information that is not related to an identified or identifiable individual. AI models are trained on large amounts of both personal and non-personal data. The quality and quantity of such training data is a key determinant of an AI model's capabilities.

Policymakers are concerned about the concentration of data resources in a small number of companies, which could result in today's most dominant digital platforms also developing monopolies in AI products and services.[89] Such concerns apply to countries as well. If a country is able to freely collect data from across the world, it can develop more competitive and capable AI models. Such capabilities can allow such a country to dominate global AI markets in addition to all other economic activities affected by AI. Notably, President Biden's executive order on sensitive personal and U.S. government data also mentions the strategic advantage that these "countries of concern" can derive from unrestricted cross-border data transfers.[90]

These concerns are expressed not only through the data sale and collection tax proposals described above, but also policies establishing data-sharing mandates. For instance, in the health sector, policies on data sharing and interoperability implemented by the Biden administration through the Department of Health and Human Services require the sharing of data with different stakeholders, including community providers and the public.[91] California has a statewide health data-sharing agreement, which requires that hospitals, insurers, and clinical laboratories share information on treatment, payment, or health care operations through a set of standards called the Data Exchange Framework.[92] Some scholars have suggested that mandatory data sharing can also be a way to break up monopolies, such as in online search.[93] The canonical example of mandatory data-sharing is the system of open banking in the European Union created by the revised Payment Services Directive (PSD-2) in

---

[89] United States, Federal Trade Commission, "Generative AI Raises Competition Concern", Technology Blog, last modified June 29, 2023. Available from https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.

[90] Executive Order 14117.

[91] "New Data-Sharing and Interoperability Mandates Create New Challenges," Avalere, last modified April 28, 2021. Available from https://avalere.com/insights/new-data-sharing-and-interoperability-mandates-create-new-challenges.

[92] Adam Hepworth, "California: Health Care Providers Must Join Statewide Data Sharing Agreement by 2024," *The National Law Review*, July 26, 2022. Available from https://www.natlawreview.com/article/california-health-care-providers-must-join-statewide-data-sharing-agreement-2024.

[93] Bertin Martens, "What Should Be Done About Google's Quasi-Monopoly in Search? Mandatory Data Sharing versus AI-Driven Technological Competition," Bruegel, last modified July 6, 2023. Available from https://www.bruegel.org/working-paper/what-should-be-done-about-googles-quasi-monopoly-search-mandatory-data-sharing-versus; Andrea Vigorito, "Government Access to Privately-Held Data: Business-to-Government Data Sharing," *European Journal of Comparative Law and Governance,* vol. 9, no. 3, pp. 237–258. Available from https://doi.org/10.1163/22134514-bja10030; Inge Graef and Jens Prufer, "Mandated Data Sharing Is a Necessity in Specific Sectors," *Economisch Statistische Berichten,* vol. 103, no. 4763 (2018), pp. 298–301. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3206685.

2018.[94] PSD-2 mandates the sharing of payments data through customer requests with other providers in the market, allowing new financial market players like payment apps to compete with large banks. The European Union's 2023 Data Act also has rules for mandatory non-personal data-sharing from private actors to the public sector and between private actors.[95] The Digital Services Act and Digital Markets Act also have rules on data-sharing and access, which apply for very large online platforms and gatekeepers, respectively.[96] These legislative efforts are a key pillar of the EU's strategy to create common European data spaces, which are ecosystems built by data infrastructures and governance frameworks and can be used by domestic and third-country businesses alike with the goal of reducing data asymmetries.[97]

In the case of data-sharing mandates, industry actors might attempt to leverage broad data flows obligations to challenge policies that limit international data transfers. As a reminder, the USMCA model of cross-border data flows obligations prohibits restrictions on the movement of data across borders. In trade law, *restriction* is traditionally interpreted as anything that has a limiting effect. If businesses can claim — and successfully convince their governments — that data-sharing mandates are so onerous that they limit their abilities to conduct business operations in the jurisdiction with such policies, they could argue that this measure constitutes a restriction on the movement on data, which would be prohibited under expansive cross-border data flows rules. As a matter of fact, the U.S. Chamber of Commerce has made precisely this claim against the EU Data Act.[98] Right now, there are no unrestricted data-transfer obligations between the United States and the EU. However, if language such as that included in USMCA were to be included in an instrument like the JSI on E-Commerce, these EU policies could be left vulnerable to international law-based corporate attacks.

---

[94] European Central Bank, "The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security," last modified March 2018. Available from https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.

[95] European Commission, "Data Act," accessed March 21, 2024. Available from https://digital-strategy.ec.europa.eu/en/policies/data-act.

[96] Luca Belli, "Data Sharing and the Delegated Act of Europe's DSA," Tech Policy Press, December 11, 2024. Available from https://www.techpolicy.press/data-sharing-and-the-delegated-act-of-europes-dsa/; "Data Sharing Obligations Under the DMA: Challenges and Opportunities," Centre for Information Policy Leadership, last modified May 2024.

[97] European Commission, "Commission Staff Working Document on Common European Data Spaces," last modified January 24, 2024. Available from https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data-spaces.

[98] Jordan Heiber and Garrett Workman, *The EU Data Act: A Misguided Policy: Forced Data Sharing & Restricted Data Flows Would Harm Economy, Undermine Cooperation*, U.S. Chamber of Commerce, last modified March 2, 2023. Available from https://www.uschamber.com/international/the-eu-data-act-a-misguided-policy.

Box 3: Examples of international data-transfer limitations regarding non-personal data

Worldwide, some laws and proposals recognize that the unrestricted cross-border transfer of even non-personal data can carry risks. In the EU, these include the Data Governance Act and the Data Act.[99] The 2022 Data Governance Act provides for the possibility of limiting the cross-border transfer, where appropriate, of some non-personal data held by public-sector bodies and other organizations in order to protect trade secrets and intellectual property rights and to protect EU citizens against de-anonymization of non-personal data.[100] The 2023 Data Act, which covers commercial entities, also limits the cross-border transfer of non-personal data in certain situations. Article 32 of the Data Act, for instance, is concerned with preventing "international governmental access to or transfer of non-personal data held in the Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member State."

Trade associations representing tech interests have claimed since these acts were first proposed that "unjustified data transfer restrictions" could be at odds with the EU's trade commitments.[101] Most of the limitations mentioned in this box are not directly connected to the protection of personal data. As such, personal data protection exceptions, such as the one proposed by the EU at the WTO, would not prevent challenges against these policies. In these cases, the EU would have to rely on the so-called "public policy" exception language, which is largely ineffective (see Box 2), to defend against a challenge to its Data Act or Data Governance Act.

Another illustrative case in relation to AI regulation is the Federal Trade Commission (FTC)'s power of disgorgement. If the FTC finds that an algorithm or model was trained on improperly obtained data, it can require that the data and the algorithm or model be deleted.[102] The FTC has used this regulatory power in the case of Cambridge Analytica, among other contexts.[103] In 2021, the FTC determined that Everbaum, a photo-storage business, had illegally developed facial recognition models based on customer data. The FTC's power of disgorgement allowed it to order Everbaum to delete the illegally held data and illegally developed models.[104]

---

[99] Kristof Van Quathem and Anna Oberschelp de Meneses, "EU Rules Restricting the International Transfers of Non-Personal Data," Inside Privacy, last modified February 1, 2024. Available from https://www.insideprivacy.com/health-privacy/eu-rules-restricting-the-international-transfers-of-non-personal-data/.

[100] Official Journal of the European Union, *Regulation 2022/868 of the European Parliament and of the Council, On European Data Governance and Amending Regulation 2018/1724 (Data Governance Act)*, Recitals 20 and 24 (2022). Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.

[101] "The European Commission Proposes New EU Data Sharing Rules, Expands Restrictions for International Transfers of Certain Data," Computer & Communications Industry Association, last modified November 25, 2020. Available from https://ccianet.org/news/2020/11/the-european-commission-proposes-new-eu-data-sharing-rules-expands-restrictions-for-international-transfers-of-certain-data/.

[102] Tonya Riley, "The FTC's Biggest AI Enforcement Tool? Forcing Companies to Delete Their Algorithms," CyberScoop, July 5, 2023. Available from https://cyberscoop.com/ftc-algorithm-disgorgement-ai-regulation/.

[103] Riley, "The FTC's Biggest AI Enforcement Tool?".

[104] Heather Federman, "Tainted Fruit: Disgorgement of Data from the FTC and Beyond," International Association of Privacy Professionals, last modified April 27, 2021. Available from https://iapp.org/news/a/tainted-fruit-disgorgement-of-data-from-the-ftc-and-beyond/.

This enforcement authority, which will be increasingly important as data disputes plague AI development, could be challenged under expansive rules banning data-transfer restrictions. For instance, if a foreign firm could claim that an order to disgorge ill-obtained data is a restriction on the flow of information it needs to conduct business, such enforcement action could be challenged under a trade agreement that replicates the USMCA model for cross-border data flows obligations.

This is not a far-fetched notion. For years, European data privacy authorities have been trying to sanction U.S.-based company Clearview due to GDPR violations committed while it built its facial recognition software. Among other enforcement actions, the French, Dutch, Italian, and Greek data protection authorities have imposed multimillion-euro penalties on Clearview; have ordered the company not to collect and process data on individuals located in these countries without a proper legal basis; and have ordered the company to delete data pertaining to individuals whose information it had processed unlawfully. So far, Clearview has refused to comply, claiming that it does not have a place of business nor any customers in the EU.[105] It is entirely likely that, were a rule banning data-flow regulation between the United States and the EU in effect, Clearview would argue that the French regulators' orders are illegal barriers to trade. Similar issues could arise with innumerable tech companies wishing to avoid compliance with the law.

The popularization of generative AI has profoundly impacted the tech policy debate worldwide. It is virtually impossible to anticipate what AI regulatory model will prevail. Yet training data is one of the key building blocks of these technologies, and rules on how it is collected, stored, used, and transferred are likely to be a fundamental component of the AI regulatory ecosystem. Trade rules banning data-transfer regulation could crucially undercut the implementation of AI policies that establish guardrails and guarantees in the development and deployment of these technologies.

[105] Natasha Lomas, "Clearview Fined Again in France for Failing to Comply with Privacy Orders," TechCrunch, May 10, 2023. Available from https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/.

FINAL REMARKS

Until recently, most discussions about the risks of imposing rules on data transfers and storage regulations have focused primarily on their impact on personal data protection. This paper explains why these risks are significant, but it also argues that such "digital trade" rules could have far-reaching consequences in the emerging data governance landscape beyond personal data protection.

Besides undercutting personal data protection regimes, "digital trade" rules that ban international data-transfer regulation and data-storage requirements could implicate government data security, tax policy, and AI regulation. Other policies that could be challenged under expansive cross-border data flows and location of computing facilities rules include:

- A Swedish law that requires a copy of accounting data to be stored locally;
- Australia's Electronic Health Records Act, which limits the foreign jurisdictions where sensitive health data can be transferred;
- An Indian insurance law that requires insurance data to be stored in domestic data centers only;
- South Korea's Land Survey Act, which prevents the unrestricted transfer of certain security-related map data outside the country;
- Potential taxes on the collection or sale of certain data, such as policies proposed in Washington state and New York;
- Data-sharing mandates, such as those included in the EU's 2018 Payment Services Directive, Data Act, Digital Services Act, and Digital Markets Act; and
- Limitations on the transfer of non-personal data outside of the EU in the Data Act and the Data Governance Act.

The data economy has only exploded in the last 20 years, and experts, policymakers, and regulators are just beginning to understand what policies are needed to ensure that these critical technologies and production processes benefit people and foster competitive markets, among other public interest goals. Given this context, policymakers and trade negotiators must exercise caution when considering binding commitments in commercial agreements that could preempt policy solutions in this developing field.

APPENDIX

The charts below compare three distinct models of international data flows commitments found in existing trade agreements with digital trade or e-commerce terms. The columns, from left to right, include the terms of the 2019 USMCA, the 2021 Mercosur E-Commerce Agreement, and the provisions from the 2022 EU-New Zealand trade agreement.

Regarding data flows and location of computing facilities language in "digital trade" agreements, there are two levels of focus: (i) the "obligation" with which countries are agreeing to conform their domestic law; and (ii) the exceptions to that obligation, which would safeguard certain policies from trade challenges.

The chart below shows side-by-side the obligations agreed to by the parties to these three agreements.

USMCA	**Mercosur**	**EU-New Zealand**
Obligations		
Art. 19.11: Cross-Border Transfer of Information by Electronic Means "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person." Art. 19.12: Location of Computing Facilities "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."	Art. 7: Cross-Border Transfer of Information by Electronic Means "Each Party shall allow the cross-border transfer of information by electronic means when this activity is for the conduct of the business activity of a person of a Party. For greater clarity, this paragraph is subject to compliance with Article 6.7." Art. 8: Location of Computing Facilities "A Party shall not require a person of a Party to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."	Art. 12.4: Cross-Border Data Flows "(...) a Party shall not restrict cross-border data flows taking place between the Parties in the context of activity that is within the scope of this Chapter, by: (a) requiring the use of computing facilities or network elements in its territory for data processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party; (b) requiring the localisation of data in its territory; (c) prohibiting storage or processing of data in the territory of the other Party; or (d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements

		in its territory or upon localisation requirements in its territory."

A thorough comparison reveals key differences in the scope of the commitments assumed by the parties of each agreement:

- While the USMCA broadly forbids any kind of government restriction on the cross-border transfer of data, the Mercosur model includes a positive obligation to "*allow the cross-border transfer of information by electronic means.*" The term "restriction" has been broadly interpreted by trade law international adjudicating bodies, which have deemed that anything that has a limiting effect could be a restriction.[106] This means that, by prohibiting any restriction on the cross-border movement of information, the USMCA model imposes a broad, open-ended negative obligation on state parties with far-reaching consequences for data regulation. Conversely, Mercosur countries did not relinquish their right to regulate or even limit data transfers in specific circumstances; allowing the movement of data does not mean that countries cannot adopt conditions to ensure that said movement respects privacy, data security, etc.

- Notably, the EU-New Zealand deal, which incorporates the EU horizontal rules on privacy and cross-border data flows, does not include a broad obligation either to avoid restrictions or allow data flows, like the USMCA and the Mercosur model do. The EU model explicitly bans the use of tools of forced localization between the signing countries while leaving room for international data-transfer regulation.

- Regarding the location of computing facilities rules in USMCA and the Mercosur deal, these terms are functional equivalents to the specific prohibitions included in the EU cross-border data flows language. This corroborates that the cross-border data flows obligations in USMCA and Mercosur go beyond prohibiting data localization measures.

- Another notable difference between the USMCA and Mercosur model relative to the EU position is that the first two establish rights for businesses, instead of only setting parameters for government action. One of the main consequences of this difference is that **the USMCA and the Mercosur rules guarantee rights for data to flow to any country as long as it is for the conduct of business by an investor or service supplier of a signatory of the agreement.** In contrast, the EU construct guarantees free flows between signatory countries only.

When it comes to the specific exceptions that have been included in these provisions, there are important differences as well. The chart below shows side-by-side the exceptions language that is supposed to provide policy space for countries to regulate in the public interest.

[106] World Trade Organization (WTO), "China – Measures Related to the Exportation of Various Raw Materials," para. 319.

USMCA	Mercosur	EU-New Zealand
Exceptions		
Art. 19.11: Cross-Border Transfer of Information by Electronic Means "This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective."[107]	Art. 7: Cross-Border Transfer of Information by Electronic Means and Art. 8: Location of Computing Facilities "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade."	Art. 12.4: Cross-Border Data Flows "For greater certainty, the Parties understand that nothing in this Article prevents the Parties from adopting or maintaining measures in accordance with Article 25.1 (General Exceptions) to achieve the public policy objectives referred to therein, which, for the purposes of this Article, shall be interpreted, where relevant, in a manner that takes into account the evolutionary nature of the digital technologies. The preceding sentence does not affect the application of other exceptions in this Agreement to this Article." "Each Party may adopt or maintain measures it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this Agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures."

The most notable differences between these models are:

[107] This exception is only applicable to the cross-border data flows obligation. The USMCA did not include a specific exception for the location of computing facilities provision.

- First, in its trade pacts based on the horizontal provisions, such as with New Zealand, the EU accompanies the cross-border data flows obligation with a largely self-judging privacy exception. A self-judging exception is by far the strongest format and is used by the United States for its FTA security exceptions. Such an exception leaves no room for a trade tribunal to second-guess a government. In this case, in the event of a challenge, a defending government does not have to demonstrate that its policy is necessary, essential, or required to protect personal data and privacy. As long as the policy is reasonably connected to data privacy objectives, the exception should trump any challenge.

- The other exceptions in these agreements are inspired by the WTO GATT and GATS general exceptions language. As explained in Box 3, tribunals have made these exceptions largely ineffective by establishing thresholds skewed in favor of commercial interests and trade liberalization over other societal goals.

- It is noteworthy that the Mercosur exception does not include a proportionality requirement, such as the necessity test, which has been fatal for many public interest policies at the WTO.

RECENT SOUTH CENTRE RESEARCH PAPERS

No.	Date	Title	Authors
173	7 February 2023	Analysis of COVID-Related Patents for Antibodies and Vaccines	Kausalya Santhanam
174	13 February 2023	Leading and Coordinating Global Health: Strengthening the World Health Organization	Nirmalya Syam
175	22 March 2023	Experiencias internacionales sobre la concesión de licencias obligatorias por razones de salud pública	Catalina de la Puente, Gastón Palopoli, Constanza Silvestrini, Juan Correa
176	29 March 2023	De dónde viene y a dónde va el financiamiento para la salud mundial	Germán Velásquez
177	18 May 2023	Policy Dilemmas for ASEAN Developing Countries Arising from the Tariff Moratorium on Electronically Transmitted Goods	Manuel F. Montes and Peter Lunenborg
178	22 May 2023	A Response to COVID-19 and Beyond: Expanding African Capacity in Vaccine Production	Carlos M. Correa
179	14 July 2023	Reinvigorating the Non-Aligned Movement for the Post-COVID-19 Era	Yuefen Li, Daniel Uribe and Danish
180	9 August 2023	Neglected Dimension of the Inventive Step as Applied to Pharmaceutical and Biotechnological Products: The case of Sri Lanka's patent law	Ruwan Fernando
181	14 August 2023	Trends, Reasons and Prospects of De-dollarization	Yuefen Li
182	7 September 2023	Multistakeholderism: Is it good for developing countries?	Harris Gleckman
183	15 September 2023	Least Developed Countries and Their Progress on the Sustainable Development Goals	Peter Lunenborg
184	15 September 2023	Promoting Jordan's Use of Compulsory Licensing During the Pandemic	Laila Barqawi
185	13 October 2023	Foreign Investment Flows in a Shifting Geoeconomic Landscape	Danish
186	14 November 2023	Patentamiento de anticuerpos monoclonales. El caso de Argentina	Juan Correa, Catalina de la Puente, Ramiro Picasso y Constanza Silvestrini
187	4 December 2023	The Global Digital Compact: opportunities and challenges for developing countries in a fragmented digital space	Carlos Correa, Danish, Vitor Ido, Jacquelene Mwangi and Daniel Uribe
188	7 December 2023	The Intersection Between Intellectual Property, Public Health and Access to Climate-Related Technologies	Lívia Regina Batista

189	21 December 2023	Status of Permanent Establishments under GloBE Rules	Kuldeep Sharma
190	24 January 2024	Implementing the Doha Declaration in OAPI Legislation: Do Transition Periods Matter?	Patrick Juvet Lowé Gnintedem
191	25 January 2024	TRIPS Waiver Decision for Equitable Access to Medical Countermeasures in the Pandemic: COVID-19 Diagnostics and Therapeutics	Nirmalya Syam and Muhammad Zaheer Abbas, PhD
192	30 January 2024	Pautas para el examen de patentes sobre anticuerpos monoclonales	Juan Correa, Catalina de la Puente, Ramiro Picasso y Constanza Silvestrini
193	2 February 2024	Desafíos actuales y posibles escenarios futuros de la salud mundial	Germán Velásquez
194	15 February 2024	Implementation of TRIPS Flexibilities and Injunctions: A Case Study of India	Shirin Syed
195	6 March 2024	Régimen de licencias obligatorias y uso público no comercial en Argentina	Juan Ignacio Correa
196	19 April 2024	Licencias obligatorias para exportación: operacionalización en el orden jurídico argentino	Valentina Delich
197	28 May 2024	Compulsory Licensing as a Remedy Against Excessive Pricing of Life-Saving Medicines	Behrang Kianzad
198	31 May 2024	What Can Cambodia Learn from Thailand and India as It Prepares to Graduate from Least Developed Country Status?	Brigitte Tenni, Deborah Gleeson, Joel Lexchin, Phin Sovath, and Chalermsak Kittitrakul
199	10 June 2024	A Toss Up? Comparing Tax Revenues from the Amount A and Digital Service Tax Regimes for Developing Countries	Vladimir Starkov and Alexis Jin
200	26 June 2024	Transforming the Non-Military Structures of Global Governance Assessing Priorities for Chapter 5 of the Pact for the Future	Harris Gleckman
201	27 June 2024	Antimicrobial Resistance: Optimizing Antimicrobial Use in Food-Producing Animals	Viviana Munoz Tellez
202	28 June 2024	Constraints to and Prospects for Sustainable Livestock Sector Practices in Argentina with Emphasis on Antimicrobial Usage	David Oseguera Montiel
203	11 July 2024	The Vaccine Industry After the COVID-19 Pandemic: An International Perspective	Felix Lobo
204	24 July 2024	Negotiating Health and Autonomy: Data Exclusivity, Healthcare Policies and Access to Pharmaceutical Innovations	Henrique Zeferino De Menezes, Julia Paranhos, Ricardo Lobato Torres, Luciana Correia Borges, Daniela De Santana Falcão and

			Gustavo Soares Felix Lima
205	30 July 2024	Foreign Direct Investment Screening for 'National Security' or Sustainable Development: a blessing in disguise?	Daniel Uribe Teran
206	28 August 2024	Equity and Pandemic Preparedness: Navigating the 2024 Amendments to the International Health Regulations	Nirmalya Syam
207	29 August 2024	Discussions on Draft Provisions on Damages in the Investor-State Dispute Settlement System in UNCITRAL Working Group III	José Manuel Alvarez Zárate
208	10 September 2024	Catalyzing Policy Action to Address Antimicrobial Resistance: Next Steps for Global Governance	Anthony D. So
209	25 September 2024	AMR in Aquaculture: Enhancing Indian Shrimp Exports through Sustainable Practices and Reduced Antimicrobial Usage	Robin Paul
210	30 September 2024	Decision 15/9 and the Nagoya Protocol: Who should get what in the Multilateral Benefit-Sharing Mechanism?	Joseph Henry Vogel, Natasha C. Jiménez-Revelles, Xavier A. Maldonado-Ramírez de Arellano
211	14 October 2024	The Implications of Treaty Restrictions of Taxing Rights on Services, Especially for Developing Countries	Faith Amaro, Veronica Grondona, Sol Picciotto
212	9 January 2025	International Regulation of Industrial Designs: The TRIPS Agreement in the Light of European Union Law	Adèle Sicot
213	13 December 2024	Navigating the WTO's Working Group on Trade and Transfer of Technology: A Critical Analysis from the Perspective of Developing Countries	Nirmalya Syam
214	15 January 2025	Application of the Bolar Exception: Different Approaches in the EU	Dmytro Doubinsky
215	23 January 2025	Assessing Five Years of the African Continental Free Trade Area (AfCFTA): Proposals on Potential Amendments	Kiiza Africa
216	27 February 2025	Will the Pact for the Future Advance a Common Global Agenda on the Challenges Facing Humanity?	Viviana Munoz Tellez, Danish, Abdul Muheet Chowdhary, Nirmalya Syam, Daniel Uribe
217	20 May 2025	Cross-Border Enforcement of Copyright: A Special Emphasis on Court Decisions and Arbitral Awards	Hany Salem
218	12 June 2025	Winds of Change: The BRICS Club of Nations Chipping Away at Western	Len Ishmael, PhD

		Dominance - The Dawn of the New South	
219	16 June 2025	Reducing the Cost of Remittances – A Priority for the Global South	Danish
220	25 June 2025	Harnessing Open Account Trade — A Major Enabler for Illicit Financial Flows from Developing Countries	Yuefen Li
221	15 July 2025	The AI Race: A Tightrope Walk Between Innovation, Inclusivity and Prosperity for All	Daniel Uribe Terán
222	16 July 2025	Designing an Independent Panel on Evidence for Action on Antimicrobial Resistance: Lessons from Selected Bodies in Global Health, Climate Change and Biodiversity	Viviana Munoz Tellez and Francesca Chiara
223	22 July 2025	Community Based Surveillance for AMR Monitoring: Significance, Requirements and Feasibility in LMICS	Afreenish Amir
224	18 August 2025	Reflections on Global Development in Times of Crisis: Arguments in Favour of an Alternate Development Paradigm	K. Seeta Prabhu
225	12 September 2025	Seven Decades After Bandung: The evolving landscape for South-South and Triangular Cooperation	Danish
226	12 November 2025	The Taxation of the Digital Economy in Practice: Digital Services Taxes and Other Measures	Natalia Quiñones, Anchal Khandelwal, Oluwole Olushola Oni, Maryam Maiyaki, Doris Malgwi, Ezekiel Swema, Nickson Omondi, Ivy Watti, Dinesh Thapa, Anne Wanyagathi Maina & Kolawole Omole
227	20 November 2025	Participation of South Centre Member Countries in the WHO GLASS: Progress and Gaps in AMR Surveillance and Stewardship Efforts	Rasha Abdelsalam Elshenawy
228	14 January 2026	UN Human Rights Council Resolutions on Access to Medicines and the Use of TRIPS Flexibilities: A Review	Nirmalya Syam
229	19 January 2026	Towards a Development-Oriented TRIPS Review Under Article 71.1	Nirmalya Syam
230	29 January 2026	The Golden Flower and the Blue Diamond: From Patent Law to Biodiversity Regimes and Guidelines	Leïla Mamoni
231	19 February 2026	AI and the Global South: Impacts, Opportunities, and Policy Approaches	Danish
232	9 April 2026	Addressing Barriers to Accessing Monoclonal Antibodies (mAbs) in Developing Countries: Challenges and Potential Solutions	Nirmalya Syam

233	14 April 2026	Access to Medicines and Intellectual Property: taking advantage of TRIPS flexibilities for post-COVID-19 resilience in Africa	Ismaelline Eba Nguema

SOUTH CENTRE

International Environment House 2
Chemin de Balexert 7-9
1219 Geneva
Switzerland

Telephone: (41) 022 791 8050
E-mail: south@southcentre.int

Website:
http://www.southcentre.int

ISSN 1819-6926