



AMERICAN
ECONOMIC
LIBERTIES
PROJECT

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

Daniel Rangel

Jai Vipra

Lori Wallach

February 2025



EXECUTIVE SUMMARY

Around the world, governments are discussing and adopting policies that regulate the ways in which data is collected, transferred, and stored, with the goal of meeting myriad public interest objectives. The regulatory drive began with the vast majority of countries adopting personal data protection regimes, most of which impose limits on the cross-border movement of data. To date, 162 countries have passed national personal data-protection laws, and 75% of all countries have adopted some limits and conditions on the cross-border transfer of data. More recently, the United States and other countries have focused on data security, including related to important geopolitical interests. Lawmakers and regulators are deploying national security measures that restrict or outright prohibit certain transactions involving sensitive data. Moreover, experts and advocates are exploring ways to adequately tax the data economy, which could be deemed as effectively curbing certain international data transfers. 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. These concerns have given momentum to data-sharing mandates and related policies.

Expansive rules in international trade agreements that impose binding restrictions on governments' abilities to regulate cross-border data flows and where data is stored run counter to these data governance efforts. For the past decade, certain tech interests have advocated 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 (cross-border data flows rules) and/or where data may be stored (location of computing facilities rules). Industry interests seek to lump all such polices together under what they consider the pejorative label of “data localization.”

In the U.S., Congress, state legislatures, the military, NASA, and the White House have all enacted policies recently that would be undermined by rules banning data transfer and storage regulation. These include:

- » ***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 moving certain types of Americans' sensitive personal information offshore so as to protect American national security and individual privacy. 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.

- » ***Cybersecurity Requirements for U.S. Cloud Computing Contractors:*** Since 2015, cloud computing service providers have been required to store defense-related U.S. government data on servers on U.S. territory. In 2023, the Federal

Acquisition Regulatory Council proposed a new regulation to require the same for non-defense-related U.S. government data.

- » ***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. This policy ordered 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 becomes effective on April 8, 2025.
- » ***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.

- » ***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.

Each of these U.S. policies fundamentally conflicts with the notion that binding international rules should prohibit governments from the regulating cross-border data flows or data storage locations. This briefing paper shows that the exceptions to such prohibitions that have been included in existing and proposed trade deals would not ensure governments’ abilities to implement these kinds of policies.

The degrees to which countries’ regulation of the data economy is impeded vary greatly depending on the scope of the trade-deal rules. The chart below compares three distinct models of international data flows rules in trade pacts. The columns, from left to right, describe the features of the 2019 U.S-Mexico-Canada Agreement (USMCA); the 2021 Mercosur E-Commerce Agreement model; and the provisions from the 2022 EU-New Zealand trade agreement.

Side-by-Side Comparison of Digital Trade Data Flows 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

Through a detailed analysis of these provisions, this policy brief shows that a potential expansion of the USMCA digital trade model would undermine existing and thwart future data-related regulation both in the United States and abroad. Indeed, changes to the USMCA rules to make them consistent with U.S.

federal and state law will be a critical part of the mandatory six-year review of the USMCA, which starts this year.

The USMCA data rules (i) establish a blanket prohibition on countries restricting cross-border movements of data, explicitly including personal

data, in addition to banning data storage and processing requirements; (ii) 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 (iii) only include a “public policy objective” exception based on deeply flawed World Trade Organization (WTO) language that has failed to preserve countries’ policy space for three decades. Both the Mercosur and the EU models have more limited restrictions on government action and allow more flexibility to regulate data transfers to meet public interest objectives.

This policy brief also explains why digital trade rules on data transfers do not remedy censorship practices in non-democratic countries and related human rights violations related to online surveillance targeting vulnerable populations by authoritarian governments. First, non-democratic countries have a poor track record of adjusting their policies to trade pact commitments. Existing WTO rules already oblige signatory countries to allow the use of their communications networks to convey information on a non-discriminatory basis. This obligation is routinely ignored by countries that block access to certain news media and other websites. Second, the policies and practices actually used by authoritarian governments to limit their citizens’ access to information or to surveil them would not be forbidden by proposed digital trade rules. Conversely, the promotion of privacy-first international instruments — such as the Convention for the Protection of Individuals with Regard to the Processing of Personal Data,

also known as Convention 108+ — is more likely to spotlight and help combat abusive practices.

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.

**AMERICAN
ECONOMIC
LIBERTIES
PROJECT**



The American Economic Liberties Project is a new, independent organization fighting against concentrated corporate power to realize economic liberty for all, in support of a secure, inclusive democratic society.

Rethink Trade was established to intensify analysis and advocacy regarding the myriad ways that today's trade agreements and policies must be altered to undo decades of corporate capture and to deliver on broad national interests.

economicliberties.us
@econliberties
info@economicliberties.us

rethinktrade.org
@rethinktrade
info@rethinktrade.org