PRESS RELEASE

Trump Administration Must Choose between Big Tech and U.S. Sovereignty as Industry Seeks to Weaponize Trade Policy to Attack Data Security, Privacy Policies in Other Nations that U.S. Has Also Adopted

Washington, D.C. – Congress and federal agencies and U.S. states have adopted the same sorts of data security and privacy policies that Big Tech lobbyists are pushing President Trump to attack as the "illegal trade barriers," a report released by Rethink Trade and the American Economic Liberties Project (AELP) revealed.

Last Friday, Trump issued an order warning other countries against regulating "American" Big Tech firms that explicitly identified "foreign legal regimes limit cross-border data flows" as the sort of policy against which tariffs, and other sanctions could be imposed.

"Pres. Trump is adamant that U.S. sovereignty and laws should never be internationally preempted by trade agreements, yet the sorts of data security and privacy policies Big Tech wants him to target for tariffs have been adopted by Congress, red States and federal agencies," **said Lori Wallach, director of AELP's Rethink Trade project.** "Big Tech's demand to weaponize trade policy to kill other nations' privacy and other data-related digital policies threatens to boomerang back again existing U.S. federal and state policies as well as policies Republicans and Democrats alike are proposing nationwide."

"This is a moment where it is really important to the reserve the power and reserve the right of the U.S. Congress to be able to protect our own citizens," **said Senator Chris Murphy (D-Conn.), who appeared at a virtual event today debuting the report.** "We have the ability to regulate the technology. We have an outstanding question before the Trump administration as to whether they carry forward the policy of the Biden administration, and we have a public out there that is hungry for Congress and the President to do the right thing and protect them in a way that has not happened. As this report will show, it's a pretty simple question. Should our democracy have the power over the tech companies, or should the billionaires and the tech companies have power over our democracy?"

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. After years of other countries adopting personal data protection regimes, most of which impose limits on the cross-border movement of data, more recently the United States has begun adopting data security measure that limit data flows and where data can be stored. This report reveals some of these policies, which are not well known after decades of inaction here

as to date 75% of all countries worldwide have adopted some limits and conditions on the cross-border transfer of data, usually related to personal privacy.

“Data transfer rules in trade agreements have significant implications for the evolving landscape of data governance, which means big stakes for national security, personal privacy, taxation, and how AI is developed and by whom,” **said Daniel Rangel, Rethink Trade’s Research Director and lead author of the report.** “While the principle of free flows of information is crucial for modern societies, trade agreements shaped by Big Tech interests that profit from controlling data often fail to find the right balance between this principle and countries' right to regulate data.”

Governments also 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 policies to ensure that smaller companies have access to this critical resource, rather than it being monopolized by incumbent tech giants, which would also implicate these rules.

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 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.”

Yet, the U.S., Congress, state legislatures, the military, NASA, and White House have all enacted policies that ban data transfer and regulate where data may be stored. 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, with the agreement providing charts and tables breaking down the systems.

Read the full report here.

Rewatch the virtual event here.

Learn more about Rethink Trade here.