Before the Department of Justice

Docket Number NSD 104

"Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons"

Written Comments from Rethink Trade

November 29, 2024

Rethink Trade thanks the Department of Justice (DOJ) for the opportunity to submit comments with regard to the implementation of 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."

Rethink Trade is a program of the American Economic Liberties Project (AELP). AELP, a non-profit research and advocacy organization, is a thought leader in the anti-monopoly movement and promotes policy changes to address today's crisis of concentrated economic power. Rethink Trade's mission is to replace decades of corporate-captured trade policies with those that can deliver broader public interest outcomes. This includes creation and support of good union jobs with workers empowered to earn decent wages, the public health and safety delivered by strong consumer and environmental protections, resilient supply chains and fair markets, and the ability for those who will live with the results to decide the policies affecting their lives.

We applaud the Biden administration's effort to enact data security policies that prevent access by malign actors to troves of U.S. citizens' personal data and government-related information. Executive Order 14117 was an important first step in ensuring that there is a federal framework to protect our personal data and national security, and the proposed regulation (the Data Security Regulation) establishes a solid system prohibiting and restricting certain data transactions that generate threats to U.S national security. However, unbeknownst to many, precisely the very policies enacted by the Data Security Regulation are the target of a set of rules being promoted by certain industry interests for inclusion in U.S. trade agreements and trade policies that would limit the U.S. regulatory authority over international data transfers. These terms, commonly known as "digital trade" rules on "cross-border data flows," severely limit governments'

authority and capacity to enact regulation that could affect the movement of data across borders. DOJ must ensure that the proposed regulation is not made vulnerable to evisceration by expansive unrestricted data transfers commitments in trade agreements.

Specifically, given that "cross-border data flows" commitments in digital trade agreements and policies could implicate data security regulation we are alarmed about the non-exhaustive nature of the exemption included in Section 202.507(a) of the proposed regulation with regard to international agreements. The current version of this section reads: "***Subparts C and D of this part do not apply to data transactions to the extent they are required or authorized by Federal law or pursuant to an international agreement to which the United States is a party*** *(…)*". The provision continues by providing a non-exhaustive list of agreements that would be a basis for transactions to be exempt from the prohibitions and restrictions in the Data Security Regulation.

We believe it is critical to clarify that the Section 202.507(a) exemption does <u>not</u> cover transactions "required or authorized" by international trade agreements. If this exemption is not clarified in the proposed manner, the goals of the data security regulation could be undermined as corporate actors could exploit data transfer rules in trade agreements to circumvent the Data Security Regulation obligations altogether.

The inclusion of cross-border data flows rules in international trade dealmaking is a very recent development. The United States is party to just two agreements that include binding commitments that prevent signatory countries from prohibiting or restricting the movement of data across borders. These agreements are the U.S.-Mexico-Canada Agreement (USMCA) and the Agreement Between the United States of America and Japan concerning Digital Trade (U.S.-Japan Digital Trade Agreement). Both of these deals have virtually the same cross-border data flows formulation: "*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.*"[1]

This obligation broadly forbids any kind of government ***restriction*** on cross-border transfer of data. 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.[2] This means that, by prohibiting any restriction on the cross-border movement of information, the USMCA and the U.S-Japan Digital Trade Agreement impose a broad, open-ended negative obligation on signatory countries with far-reaching consequences for data regulation. Moreover, this obligation guarantees 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. This means that, for instance, a Japanese business is empowered to move U.S. data to any country under the U.S.-

[1] USMCA Article 19.11. Article 11 of the U.S.-Japan Digital Trade Agreement has almost the same language.
[2] WTO, "China – Measures Related to the Exportation of Various Raw Materials," para. 319.

Japan deal, including to the foreign countries of concern identified in the proposed regulation. In other words, the obligation is not limited to guaranteeing data flows between the signatory countries.

If the term "international agreements" in Section 202.507(a) of the Data Security Regulation is interpreted to include trade agreements with unrestricted data transfer commitments such as the ones noted here, the goals and effectiveness of this policy would be crucially undercut. Investors or service suppliers of a signatory country could claim that transactions that would be otherwise prohibited under the Data Security Regulation are allowed under the respective trade-agreement "cross-border data flows" obligation. This would allow them to argue that the transactions are authorized by an international agreement to which the United States is a party and, consequently, exempted from the Data Security Regulation.

DOJ must ensure that the proposed regulation is not made vulnerable by expansive unrestricted data transfers commitments under trade agreements. To that end, the final version of Section 202.507(a) of the Data Security Regulation must clarify that transactions covered by trade or commercial agreements are not covered by the exemption.

This action is unlikely to upset our trading partners or generate trade irrtants because, fortunately, both the USMCA and the U.S.-Japan Digital Trade Agreement have strong, self-judging national security exceptions.[3] Japan, Mexico, and Canada have no expectation that the United States cannot restrict data flows for national security reasons because these exceptions would preserve the right for the U.S. government to restrict flows. These exception could be invoked if a party of one of these agreements challenges the exclusion of trade agreements from the list of international agreements that exempt transactions from the prohibitions and restrictions proposed by the Data Security Regulation. The United States would be on strong footing in any potential dispute under these agreements with regard to data security policies.

However, proposals on "cross-border data flows" rules have arisen in other trade negotiations in which the United States is engaged. Most notably, the talks launched by a group of members of the World Trade Organization (WTO) known as the Join Statement Initiative (JSI) on E-Commerce has included negotiations to establish international data flows provisions.[4] Countries of concern identified in the Data Security Regulation, such as the People's Republic of China and the Russian Federation, are active participants in these WTO JSI discussions.

[3] Article 4 of the U.S.-Japan Digital Trade Agreement establishes the following security exceptions: "Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests." USMCA Article 32.2 includes the same language.

[4] See: https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

There is no guarantee that any deal coming out of these negotiations would include a self-judging national security exception, such as the one inserted in the existing U.S. deals with data flows commitments. As a matter of fact, in July 2024 the countries leading these negotiations published a "stabilized text" that is expected to work as a platform for negotiations on this subject in the future. This text has a security exception that does not safeguard the policy space required by the United States to adopt data security rules as the USMCA or the U.S.-Japan agreement do. The security exception in this text merely states that the corresponding security exceptions of the WTO General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (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' ability to successfully use the WTO security exceptions to defend domestic policies is limited 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 exception to defend various China-related trade policies. Notably, the U.S. government has sought to include a meaningful national security exception similar to that in the USMCA or U.S.-Japan deals in the WTO E-Commerce JSI, but to date this efforts has been rejected.

The WTO JSI "stabilized text" does not include rules on data transfers, however that is only because the countries have been unable to agree on specific language in this area to date. The text does include an exception related to privacy and data flows, which reflects the expectation that data flows obligations will be included as the talk continue. In 2019, the U.S. government submitted the language quoted above that strictly limits government regulation of data flows to be included in the WTO JSI. U.S. government discussions of emerging data security concerns have proceeded since 2019. In 2023, the Biden administration withdrew U.S. support for this proposed obligation. However, other countries continue to support it. And, industry interests continue to push for its inclusion in agreements worldwide.

The potential risks coming out of the WTO E-Commerce agenda and other digital trade negotiations require DOJ to remain vigilant to ensure that any agreement resulting from these processes to which the United States could become a signatory, does not affect U.S. data security initiatives.

To conclude, we commend DOJ for advancing the critical goal of safeguarding U.S. citizens' personal data and U.S. government information. We urge the Department to address the risk related to trade agreements in the final version of the regulation by explicitly excluding trade agreements or other "digital trade" agreements from its definition of international agreements in

Section 202.507(a) exemption. We urge DOJ to remain vigilant with respect to the evolving threats posed by industry efforts to include of international data transfers commitments in trade agreements.