



The Honorable Joseph R. Biden
President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

March 10, 2023

Dear President Biden:

As diverse organizations working to ensure digital privacy protection and data security, we write to express concern about “digital trade” negotiations related to the proposed Indo-Pacific Economic Framework (IPEF). It is essential that digital trade rules do not undermine Congress’s ability to protect online privacy or data security. That is why we urge you not to replicate the Big-Tech-favored terms that were slipped into the U.S.-Mexico-Canada Agreement (USMCA) and the Trans-Pacific Partnership (TPP) that cede control of our personal data to firms, including rights to move, process, and store personal data wherever they choose.

We appreciate your comments in your State of the Union address underscoring that “it’s time to pass bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data that companies collect on all of us.” Our organizations have consistently fought for these very goals, supporting the critical U.S. state and national initiatives needed to allow the United States to catch up to, and surpass, the online privacy protections people in other countries enjoy.

As your U.S. Trade Representative, Ambassador Katherine Tai, noted in her 2021 speech on digital trade, a new approach is necessary. However, we understand from policymakers and others who have reviewed the draft IPEF digital trade text circulated in February that it includes problematic terms that provide Big Tech firms control of our personal data and strictly limit government action to protect our fundamental rights. We know that Big Tech companies are advocating for an approach to digital trade that would derail the online privacy initiatives coming from Congress and your administration.^[1]

In effect, these interests are promoting a form of international preemption. Their goal is to use closed-door “trade” negotiations to secure binding international “digital trade” rules that limit, if not outright forbid, governments from enacting or enforcing domestic policies to counter Big Tech privacy abuses and online surveillance. In fact, many of these rules have nothing to do with trade.

Rather, they would establish new binding legal restrictions on the U.S. government's ability to regulate what tech firms can do with Americans' personal data. Such "digital trade" terms are a stealthy backdoor effort to derail necessary digital governance initiatives here and around the world. Until the TPP's E-Commerce Chapter and then the USMCA, U.S. trade pacts with digital rules simply did not include any rules on data flows and the location of computing facilities, much less the extreme guarantees established in USMCA Article 19.11 (Cross-Border Transfer of Information by Electronic Means) and Article 19.12 (Location of Computing Facilities).

The goals and terms of policies like the American Data Privacy and Protection Act and My Body, My Data Act of 2022, or similar legislation, could be undermined by these rules. Firms can simply evade obligations to eliminate private data per users' requests or minimize collection by transferring data to another firm in a jurisdiction where U.S. law enforcement cannot reach. Offshore processors, similarly, would be able to sell data onward to firms located in a country where no protections apply. Yet attempts by Congress or regulatory agencies to address these issues through legislation or rulemaking likely would conflict with the USMCA-style rules prohibiting government regulation of data that industry seeks for the IPEF and other pacts.

These terms would also directly forbid security initiatives such as the Protecting Americans' Data From Foreign Surveillance Act. This bipartisan bill would enact export controls on transferring certain personal data offshore when it threatens U.S. national security. Only certain countries would be eligible to receive Americans' personal data without being subject to controls and flows to some nations would be wholly banned, both of which violate the USMCA-style rules sought for IPEF. The industry-favored rules would also forbid proposals to require sensitive infrastructure data to be held on U.S. servers and various proposals to limit flows of Americans' data to countries where it would likely be rendered insecure or misused, such as China.

We recognize that data flows are critical for the internet's function. However, trade pacts must not include terms that limit government regulation of data flows related to privacy protections or data security. In addition, trade pacts must provide policy space and include specific exceptions for government action to protect privacy and include carveouts that exclude from the rules especially sensitive types of data. We understand that the draft IPEF digital text does not include these essential safeguards. We understand that the exception language is not broad enough to safeguard the policy space needed for essential digital governance policies and that it replicates controversial terms from the General Agreement on Trade and Tariffs' (GATT) general exceptions. (These GATT exceptions have failed in all but two of 48 attempted uses, so this language cannot be relied upon to provide meaningful exceptions to digital trade rules otherwise forbidding government regulation.)

Given the draft U.S. IPEF digital trade text would create untenable conflicts with privacy and data security policies being promoted by your administration and Congress, we urge you not to submit this text and instead to work with privacy advocates in Congress and outside to create IPEF proposals that are consistent with the public interest.

Finally, that such terms would be established through closed-door international negotiations is extremely troubling. We join the hundreds of U.S. organizations that have urged the

administration to open the process of these negotiations. Everyone who will live with the results should be able to see the U.S. digital proposals for IPEF and see the drafts of the IPEF digital chapter as talks proceed. That 500 official U.S. trade advisors who mainly represent corporate interests have access to the draft IPEF digital text, yet the leading U.S. organizations advocating for online privacy and data security must rely on the broad characterizations from policymakers and others under confidentiality constraints is unacceptable.

We want to work with you, Mr. President, to deliver the privacy protections you spotlighted in your State of the Union speech. We are relying on you to ensure that the IPEF and other trade pacts do not undermine our common online privacy goals.

Sincerely,

American Economic Liberties Project
Center for Digital Democracy
Center for Economic Justice
Common Sense Media
Consumer Action
Consumer Federation of America
Demand Progress Education Fund
The Electronic Privacy Information Center (EPIC)
Fairplay
Fight for the Future
The Greenlining Institute (GLI)
National Consumers League
NETWORK Lobby for Catholic Social Justice
Open MIC (Open Media and Information Companies Initiative)
Public Citizen
Public Knowledge
Rethink Trade
Trade Justice Education Fund

cc:

Secretary of Commerce Gina Raimondo
U.S. Trade Representative Katherine Tai
National Economic Council Director Lael Brainard
National Security Advisor Jake Sullivan