CORRECTING THE RECORD

Myths and Facts about Digital Trade Rules

Myth: Digital Trade Rules Only Benefit 'Big Tech'.

Fact: Digital trade rules benefit firms from all sectors of the economy, especially SMEs.

Small and medium-sized enterprises (SMEs) are prime beneficiaries of digital trade rules, which facilitate their ability to reach foreign markets online:

- More than 80% of top grossing apps are made by small companies.
- Over 300,000 companies are active in the mobile app market in the United States, participating in an "app economy" estimated to be worth $1.7 trillion.
- SMEs comprised 70% of the companies using Privacy Shield, a key mechanism allowing U.S.-EU data transfers.

All these firms need to transfer data, and few can afford to invest in computing facilities in every market they serve - issues that trade rules address.

By preventing a range of discriminatory barriers, digital trade rules help small businesses "achieve scale without mass" and expand their footprint with fewer resources. Foreign markets represent a key area for growth for small businesses enabled by digital services—the U.S. Census Bureau has estimated that 97.4% of the more than 277,000 U.S. companies that exported goods in 2021 were SMEs, which in turn contributed 34.6% of the country's $1.5 trillion merchandise exports. These firms typically use digital technologies to access foreign markets and thus distortive foreign policies can have a disproportionate effect on their growth and job-creating potential.

Myth: Digital Trade Rules Hurt U.S. Workers.

Fact: Digital trade rules sustain broad-based, high-quality U.S. jobs.

Quality jobs supported by digital trade permeate the U.S. economy, encompassing firms both large and small. Some of the biggest beneficiaries of the digitalization of the economy are traditional sectors—pharmaceutical development, health care, transportation, travel, and agriculture—supporting technology workers whose wages are 125% higher than the median national wage in the U.S. The export potential of digitally-intensive industries, and the employment they support, benefit from a fair and predictable rules-based framework for trade: government data indicates that the digital economy in 2021 generated $3.70 trillion in output, or 10.3% of total U.S. GDP, accounting for 8 million jobs, over $1.24 trillion in total compensation, and a persistent trade surplus (most recently of $300 billion). It is in our national interest to leverage this strength, not constrain it.

Myth: Digital Trade Rules Undermine Countries' Right to Regulate in the Digital Space.

Fact: Digital trade rules do not prevent governments from regulating effectively and appropriately.

Governments' right to regulate is explicit in trade agreements, with rules affecting not whether a country can regulate but how. Digital trade rules developed to date in agreements like USMCA (support of data flows, constraints on localization and discriminatory treatment) are narrowly targeted to provide guardrails around only the most unreasonably trade-restrictive practices, leaving most economic activity wholly in the domain of domestic regulation. Such a targeted approach avoids governments pursuing policies that unfairly discriminate in favor of local suppliers, while taking into account national policies and practices. Trade rules include flexibility based on legitimate exceptions (privacy, security, public morals, etc.). In the face of a country invoking such an exception, a trading partner must demonstrate that there is a reasonably available approach that achieves the regulatory goal – goals that a country independently sets. Thus, the key effect of a negotiated trade rule is a level of accountability between trading partners based on shared values and ensures that regulation in narrowly identified areas is developed pursuant to fair and transparent processes.

Myth: Digital Trade Rules Undermine Consumer Privacy and Consumer Protection.

Fact: Digital trade rules can enhance consumer protection and privacy rights.

A key innovation in recent U.S. digital trade policy is undertaking binding obligations to protect consumers generally and privacy in particular—putting this goal front and center as not only a legitimate regulatory objective, but one that countries must implement. The USMCA and the U.S.-Japan Digital Trade Agreement each included such provisions, incorporating into trade rules a binding obligation as well as OECD guidance on how to implement an effective privacy regime. In USMCA, the Parties expanded on this by also referencing the U.S.-championed APEC Privacy Framework.

At the heart of the traditional U.S. approach has been the well-established norm that privacy protections do not depend on location, and that protections can, with the right mechanisms, travel with data, minimizing the need for overly restrictive constraints on cross-border data flows. Not only are private sector entities fully capable of instituting mechanisms that can reflect the highest levels of protection different countries may set, but democratic governments have also developed principles governing governmental access to data, such as the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities. Such principles can be incorporated into trade frameworks (e.g., ongoing IPEF negotiations) demonstrating that trade rules can enhance, not undermine privacy.

Myth: Data Localization Rules are Needed to Protect Privacy and Ensure Government Access.

Fact: Data localization mandates do not strengthen privacy or security and can actively undermine these goals.

Data localization requirements do not, in and of themselves, enhance data privacy or security. While certain sensitive data (e.g., national security data, health data, and financial information data) merits additional safeguards, such safeguards (e.g., encryption, multi-factor authentication) can be applied irrespective of location and do not require data localization. To the extent that governments need access to data for regulatory or law enforcement purposes, and where the U.S. cannot be ensured such access, identifying specific unacceptable locations would be consistent with the rule. But, a general prohibition on foreign storage is unnecessary.

Data localization requirements in specific markets often have a direct and negative impact on U.S. suppliers: such requirements typically result in superfluous investment, often in countries with less robust cybersecurity practices than performed in the United States. Accordingly, forced localization can demonstrably weaken security, since the proliferation of redundant facilities opens an additional "attack surface" for bad actors.

Apart from the security, the economic impact is obvious. The United States leads the world in data processing and storage capacity, so any requirement to move such capacity to a foreign location to serve that market undermines the clear competitive advantage enjoyed by U.S. exporters of services based on secure processing and storage.

Myth: Digital Trade Rules Will Hurt U.S. Jobs.

Fact: Jobs in digitally-intensive industries are growing.

Over the past decades, digitally-intensive job growth is responsible for a net gain of over 15 million jobs. This growth remains strong, with unemployment rates half those of the economy generally—supported by robust digitally-enabled exports. Even the one target of trade critics, call-center jobs, do not support the offshoring narrative: call center jobs have actually increased in the past decade, from 2.3 to 2.8 million. In short, trade rules that support the U.S. competitive advantage in the digital economy will help ensure strong U.S. job growth going forward; and a turn to localization and other protectionist measures (as seen in the EU and China) will only diminish it.

Myth: Digital Trade Rules that Prohibit the Disclosure of Source Code Undermine a Regulator's Ability to Investigate Harms.

Fact: Digital trade rules strike the right balance between protecting trade secrets and the public interest.

Regulators may need access to source code in limited cases, and these cases can be addressed in trade rules, as was done in USMCA, balancing such access against the harms to trade secrets and cybersecurity protections. Rules limiting access to source code are not designed to, and do not in practice, protect companies from regulatory oversight or enforcement actions. Those goals generally can be addressed through robust testing, and does not require access to source code. Regulating against commonly identified harms (bias, inequity, and other forms of discrimination) is fully consistent under digital trade rules. And, where evidence of harms emerges, particularly when it is intentional (e.g., in the motor vehicle emissions cases of a decade ago, or financial market manipulation), the rules accommodate such need for access—subject to requirements under the law to protect the trade secrets and other confidential business information. Expanding the scope of regulatory access to source code puts U.S. companies at significant risk in many markets that do not have the robust trade secret protections of the United States. To this end, trade agreements should not create new access rights to governments or third parties that are not available under existing Parties' law.

Myth: Non-Discrimination Rules Hinder Enforcement of Existing and New Anti-Monopoly Laws.

Fact: Prohibiting discrimination on the basis of nationality is a worthy goal that does not implicate robust competition enforcement

Critics of digital trade rules have asserted that a 20-year-old rule preventing discrimination against digital products undermines efforts to enforce or enhance competition law. The digital products rule[1] extends a 75-year-old "national treatment" rule common in trade agreements,[2] that is applicable to physical products, to their digital counterparts. Based on this rule, a country would be prohibited, for example, from imposing a tax on foreign software that was downloaded from abroad that it does not also impose on domestic software (i.e., creating a preference for domestic software). This rule has no more bearing on legitimate competition law than its older goods-rule analogue. Critics are erroneously conflating how a government treats a supplier generally with how that supplier's products are treated in comparison to those of its competitors.

Regardless of whether new competition-inspired regulation is justified, measures seeking to constrain the behavior of specific suppliers (e.g., Europe's Digital Markets Act, Korea's App

[1] e.g. USMCA 19.4, available here: https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf
[2] i.e., Article III-4 of the General Agreement on Tariffs and Trade, available at https://www.wto.org/english/docs_e/legal_e/gatt47_01_e.htm

store legislation) do not typically result in creating explicit "preferences" for domestic products, the target of digital non-discrimination rules.[3] Rather, these regulations typically seek to constrain specific conduct of specific firms.

CCIA has raised compliance concerns with the digital product rule in the context of efforts to impose payment obligations on U.S. digital platforms for hosting or indexing news content in Canada and Australia. The problematic discrimination identified in these instances is not vis-a-vis the internet platforms but, rather, competing foreign news products. None of this is relevant to any U.S. domestic conversation, since trade rules do not constrain burdens that the United States may choose to apply to its own suppliers.

[3] There is a separate question of whether competing domestic firms as a whole gain preferential treatment by virtue of being excluded from the scope of such regulations. That is a legitimate inquiry under the analogous national treatment rules for services, but such inquiry does not does not require analyzing treatment of those domestic firms' products.