Trade Barriers for Digital Exports
Identifying Threats to U.S. Leadership in Global Digital Trade

Internet-enabled trade in goods and services is a driver for U.S. economic growth, but firms are facing growing barriers that hinder their ability to access foreign markets—both through exports and in-country sales. The U.S. should lead in setting rules for digital trade through new and existing international partnerships. Identifying and addressing key threats, and leveraging trade partners in this effort, is critical to achieve this goal.¹

What’s At Stake?

Digital trade is driving broad benefits to U.S. companies and domestic workers, resources, and economic value.

<table>
<thead>
<tr>
<th>A digital economy that generated²</th>
<th>A digital economy that generated³</th>
<th>U.S. Generated Exports Abroad⁴</th>
<th>Essential part of U.S. export strength⁵</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.14T</td>
<td>10.2%</td>
<td>684B</td>
<td>77%</td>
</tr>
<tr>
<td>OF VALUE ADDED IN 2020</td>
<td>OF TOTAL U.S. GDP in 2020</td>
<td>GLOBALLY IN ICT SERVICES</td>
<td>of all U.S. services exports in 2021</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>7.8m JOBS IN U.S.</td>
<td>1.09T</td>
<td>300B TRADE SURPLUS IN INDUSTRY</td>
<td>Digitally-deliverable services represented</td>
</tr>
<tr>
<td></td>
<td>IN ANNUAL COMPENSATION</td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

In the face of global economic threats posed by the COVID-19 pandemic U.S.-based digitally-deliverable services and e-commerce services, persisted and performed robustly. Internet-enabled services have facilitated domestic and cross-border communications, streamlined the exchange of services and goods, and enabled government and business activity to continue remotely. These services will only increase in importance as a source in economic growth, prosperity, and consumer welfare.

³ https://apps.bea.gov/iTable/?reqid=62&step=6&isuri=1&tablelist=359&product=4
⁵ This October 2022 summary draws upon the annual submission of CCIA to the Office of the U.S. Trade Representative, as U.S. trade officials prepare the 2023 National Trade Estimate Report. https://www.ccianet.org/library-items/ccia-comments-2023-national-trade-estimate-reporting/
Efforts to Extract and Redistribute Revenue of U.S. Digital Services Among New Digital Trade Barriers

International markets continue to present the most significant growth opportunities for major U.S. companies, even as international competition has grown. However, a troubling trend is emerging: governments adopting thinly-disguised mechanisms for extracting and redistributing revenues and resources, designed to target U.S. firms and benefit domestic industries. This is evident in policies seeking to transfer revenue from digital platforms to news organizations and from content and application providers to ISPs in the form of so-called network usage fees. Similarly, policies in several economies are seeking to transfer commercially-obtained data and analytics from U.S. firms to their domestic competitors. At the same time, there is a rise in authoritarian governments’ control of Internet services to restrict speech and undermine security of users while specifically targeting U.S. companies and harassing their employees to restrict firms’ ability to operate freely.

Regulatory frameworks and policy agendas imposed pursuant to these goals will undermine U.S. leadership in the global economy, pose conflicts with international trade commitments, disrupt the global nature of the free and open Internet, and impair the U.S. capacity to export digital services. Isolationist and protectionist digital policies are no longer limited to China and Russia. Traditional U.S. partners such as the European Union, Korea, and Canada are now also seeking to draw up digital borders, increasing the need for robust U.S. engagement.

Such engagement with trading partners should include addressing concerns, pursuing new trade agreements and leveraging commitments under existing trade frameworks to open up foreign markets and ensure that countries fulfill their obligations.

2022 Key Threats


Cross-border data flows underpin digital trade. Localization mandates for data and infrastructure are intensifying globally and hinder U.S. exporters from expanding into new markets. The U.S. should work with trading partners to both remove and prevent future barriers to cross-border data flows and discourage data localization mandates, encouraging partners to model strong commitments on the digital trade chapter in USMCA. Increasingly, countries are pursuing data protection laws, which often fail to provide for clear rules to transfer data or impose onerous obligations for data processing and storage.

2. Tightening Grip on Internet services from Authoritarian Regimes.

U.S. firms face hostile environments in several markets which impedes company operations. Among the most explicit barriers to digital trade are the outright filtering and blocking of U.S. Internet platforms and online content. Some countries are also pursuing content regulations that grant the governments extensive powers to compel companies to comply with takedown orders, often accompanied with new levels of intimidation for local employees. Key threats include India’s expanded oversight of online content and services, Russia’s censorship laws that have intensified during its invasion of Ukraine, and Turkey’s increased obligations on the use and operation of social media.
2022 Key Threats

3 Forcida Payments Between Online Services and Local Incumbents in Telecommunications and News Publishing.

Governments are pursuing rules to force U.S. online services providers into paying local incumbents through mandatory negotiations. In lieu of free market negotiations between online services suppliers and local industry players, these frameworks implement an obligation for platforms—targeting a select few U.S. firms—to choose between paying powerful entities in local markets or exiting the market. Examples of these rules include Australia’s News Media Bargaining Code, Canada’s Bill C-18, and Czechia’s proposed rules forcing online platforms to negotiate payments for news content shared through their services; and South Korea proposals to force select content and application providers to pay domestic telecommunication service providers for delivering traffic to their Internet subscribers.

4 Discriminatory Platform Regulation Based on Ill-Defined Market Analysis.

A general but ill-defined desire for “platform regulation”, unsupported by evidence of consumer harm, is spurring digitally-focused ex-ante regulation around the world, including the EU, Japan, South Korea, and Australia. In some cases, platform regulation serves as a backdoor for industrial policy dressed up as competition policy and typically employ thresholds designed specifically to target leading U.S. Internet services. Such regulatory approaches depart from best practices of seeking general rules of industry-wide application, as opposed to targeting individual companies, absent credible evidence of market failure or consumer harm. Additionally, rather than being developed through highly prescriptive legislation, best practices also suggest that they be developed pursuant to a transparent rulemaking process that follows global norms.

5 Undermining Security in Communications.

Tools like strong encryption, critical to a trustworthy digital ecosystem, are common on devices such as smartphones and are increasingly deployed end-to-end on communications services and browsers, for both consumers and businesses. Many countries, at the behest of their national security and law enforcement authorities, are considering or have implemented laws that mandate access to encrypted communications—thereby undermining business and consumer security. For industrial policy reasons noted above, some platform regulation proposals also seek to mandate data sharing and access to core technical and operational functionality of devices. Additionally, rules various countries have implemented or are considering seek to undermine virtual private networks, compel interception of messages on OTT communications services, and require unique local cybersecurity standards, all of which further harm digital security. Such rules ultimately restrict U.S. firms from operating in foreign markets since they necessitates weakening their goods and services globally, and preclude the use of standardized, scalable technologies.

This October 2022 summary draws upon the annual submission of CCIA to the Office of the U.S. Trade Representative, as U.S. trade officials prepare the 2023 National Trade Estimate Report. View the submission here: https://www.ccianet.org/library-items/ccia-comments-2023-national-trade-estimate-reporting/