



# Defending American Tech in Global Markets

ROBERT D. ATKINSON AND HILAL AKA | DECEMBER 2025

---

“Non-tariff attacks” on U.S. tech companies are not just tax and regulatory hurdles—they are also eroding America’s strategic edge. Washington must identify, deter, and counter these measures in order to prevent ceding U.S. technology leadership to other nations.

---

## KEY TAKEAWAYS

- Foreign governments are deploying a new trade weapon against leading U.S. tech companies: “non-tariff attacks” (NTAs).
- NTAs are not legitimate taxes and regulations, but rather discriminatory operational constraints and revenue extraction tools that precisely target leading U.S. tech companies.
- U.S. strategic innovation is driven by major private firms. Discriminatory attacks on them erode America’s industrial base and undermine its technology leadership and global competitiveness by diverting capital away from research and development.
- As U.S. firms are hampered by these attacks, China’s state-backed champions expand unchallenged in global markets, seizing the competitive advantage America is losing.
- Washington therefore must treat NTAs as an urgent threat to U.S. technology leadership.
- That requires systematically tracking their impact, elevating them to the highest priority in trade negotiations, and countering them through coordinated diplomacy, trade enforcement, and retaliation.

## CONTENTS

Key Takeaways.....	1
Introduction.....	3
The Anatomy of Attacks on U.S. Tech .....	4
Nonmarket Nature of the Attacks.....	5
Extraction Tools .....	5
The Targeting Pattern.....	6
Offensive Strategy.....	6
The Cost of Attacks on U.S. Tech.....	7
Cost for the United States.....	7
Tech Leadership .....	7
Geopolitical Influence .....	8
Cost for the American Tech Industry .....	8
Fines and Fees .....	8
Compliance Burden.....	8
Opportunity Cost.....	9
Policy Recommendations .....	10
Identify and Assess .....	10
Consider National Competitiveness in Antitrust.....	10
Require Periodic Economic Impact Assessments of NTAs .....	11
Document Impact on SMEs and Innovation Ecosystem .....	12
Engage and Negotiate With Leverage .....	13
Make Digital Barrier Removal a Priority in All Trade Negotiations.....	13
Leverage AI Investments and Partnerships as Systemic Incentives .....	14
Prioritize Digital Policy in Development Finance Corporation Investments.....	15
Restore and Expand Digital Policy Capacity Building for Developing Countries .....	16
Counter and Deter.....	16
Prevent NTAs from Becoming Global Norms Through Multilateral Forums.....	16
Launch Section 301 Investigations Into Major NTAs .....	17
Re-engage in Multilateral Digital Trade/Digital Economy Disciplines Outside the WTO .....	18
Implement Reciprocal Measures With Escalating Consequences.....	19
Endnotes.....	21

## INTRODUCTION

In 2024 alone, the European Union imposed \$6.7 billion in fines on American technology companies, an amount equivalent to nearly 20 percent of what the EU collected in tariff revenue, demonstrating how regulatory fines have become a significant revenue extraction mechanism.<sup>1</sup> Over 80 percent of fines collected under the EU General Data Protection Regulation (GDPR), Europe's comprehensive privacy law, have been issued against U.S. firms.<sup>2</sup> This pattern extends beyond Europe: American tech companies have faced fines totaling more than \$30 billion globally over the past decade for antitrust or data protection issues.<sup>3</sup> Yet, fines are just one weapon in an expanding arsenal: governments worldwide now deploy discriminatory policies, such as digital services taxes (DSTs), forced data localization mandates and technology transfers, and operational restrictions that constrain American companies' innovation capacity.

These measures constitute a new category of trade weapon: non-tariff attacks (NTAs). Unlike tariffs or conventional barriers that limit market access, NTAs erode the global competitiveness of targeted firms through regulatory fines, DSTs, forced localization requirements, and operational constraints. They are framed as legitimate domestic policies, but their function is to weaken American technology leadership in favor of domestic champions.

The impact extends beyond individual companies. NTAs undermine U.S. competitiveness and national security in two ways: They displace American firms and reduce market share, harming U.S. jobs and the U.S. trade balance, and they divert capital from research and development (R&D) into fines, localization, and compliance. A single €2.4 billion (\$2.79 billion) penalty is equivalent to Google's entire investment in a major Indiana data center.<sup>4</sup> When compliance costs divert tens of billions of dollars annually from R&D, the drag on innovation becomes clear.

As the Trump administration addresses global trade imbalances stemming from unfair foreign policies and practices, recognizing and countering NTAs should be a priority. The United States needs a systematic strategy to identify, document, prevent, and respond to these measures. Foreign governments must face concrete consequences from the U.S. government, not just the occasional scold or flaccid threat. The Trump administration needs to continue and expand its efforts to make it clear that these attacks will be met with forceful resolve.

The administration should take decisive action to counter these attacks, as follows.

### Identify and assess:

1. **Incorporate competitiveness into antitrust.** Require Department of Justice (DOJ) and Federal Trade Commission (FTC) to consider international competitive effects when pursuing enforcement actions against U.S. tech firms.
2. **Track and quantify NTA impacts.** Direct the United States Trade Representative (USTR) to publish quarterly economic impact assessments documenting fines, compliance costs, and market losses.
3. **Document impact on small and medium-sized enterprises (SMEs) and the innovation ecosystem.** Expand Commerce Department surveys to capture how NTAs affect startups, venture capital, and acquisition pathways.

### Engage and negotiate:

4. **Make digital barrier removal a priority in all trade negotiations.** Require binding commitments against discriminatory digital regulations with identical enforcement as traditional violations.
5. **Leverage artificial intelligence (AI) investments and partnerships as systemic incentives.** Condition U.S. AI partnerships and cloud investments on verifiable commitments to nondiscriminatory digital policies.
6. **Prioritize digital policy in Development Finance Corporation (DFC) investments.** Direct DFC to favor investments in countries that are maintaining open digital policies.
7. **Restore and expand digital policy capacity building.** Expand the State Department's Bureau of Cyberspace and Digital Policy to provide technical assistance on market-friendly digital strategies.

### Counter and deter:

8. **Prevent NTAs from becoming global norms through multilateral forums.** Actively challenge efforts to legitimize discriminatory policies at the Organization for Economic Cooperation and Development (OECD), G7, G20, United Nations (UN).
9. **Launch Section 301 investigations into major NTAs.** Investigate the EU's Digital Markets Act (DMA), Digital Services Act (DSA), and discriminatory GDPR enforcement with readiness to impose reciprocal measures.
10. **Re-engage in multilateral digital trade disciplines.** Join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and pursue agreements that prohibit data localization and protect cross-border data flows.
11. **Implement reciprocal measures with escalating consequences.** Establish a structured framework wherein countries face predictable consequences within one quarter after being cited if they fail to address NTAs.

## THE ANATOMY OF ATTACKS ON U.S. TECH

NTAs represent a new form of trade barrier. Tariffs tax imports at the border, raising prices and limiting market access. Non-tariff barriers (NTBs)—such as local technical standards, licensing requirements, and quotas—restrict trade through regulatory mechanisms rather than direct taxes, often justified as safety or quality measures while serving protectionist goals. NTAs represent a third, more sophisticated category: policies disguised as legitimate domestic regulations but precision-engineered to target specific foreign firms rather than necessarily protect domestic industries. NTAs actively extract resources, force technology transfers, and degrade the competitive advantages of selected foreign companies—often without viable domestic alternatives to protect.

NTAs manifest through four primary mechanisms:

1. Nonmarket interventions

2. Extraction mechanisms to capture fiscal revenues, physical infrastructure, and proprietary business assets
3. Precision targeting uses engineered thresholds and selective enforcement
4. Offensive degradation strategies to undermine competitive advantages through forced interoperability, technology disclosure mandates, and operational constraints

## Nonmarket Nature of the Attacks

What distinguishes NTAs from legitimate regulation is their departure from market-correcting principles. For example, unlike value-added taxes (VATs) on consumption, a DST taxes gross revenue rather than profits, so companies pay even when they are losing money. Many DSTs also set high revenue thresholds—such as €750 million (\$870 million) worldwide—aimed at targeting American tech leaders while excluding smaller domestic competitors. And DSTs violate existing international tax agreements, such as the OECD guidelines on international taxation.<sup>5</sup>

These measures don't correct market failures; they penalize successful competitors in foreign markets. When countries lacking competitive domestic cloud industries impose data localization requirements, they're not even achieving protectionist goals; they're forcing American companies to build expensive infrastructure as the price of doing business.

The European Union's DMA imposes preemptive obligations on “gatekeepers,” a group of seven digital companies—of which five are American—selected based on revenue, market capitalization, and user-base thresholds without evidence of consumer harm or benefit.<sup>6</sup> Its interoperability mandates force Apple to open its iOS features to third-party devices while degrading security and user experience. Rather than correcting market failures, these requirements transfer value from successful platforms to their competitors.

## Extraction Tools

These attacks extract value through three primary channels: financial penalties, physical infrastructure, and proprietary business assets.

Direct financial extraction operates through regulatory fines based on global revenue rather than local harms, and through DSTs on gross revenue rather than profits. Turkey's proposed DMA authorizes penalties up to 20 percent of global revenue.<sup>7</sup> India can fine up to 10 percent of a firm's average turnover.<sup>8</sup> Brazil's proposal allows fines of 20 percent of Brazilian turnover.<sup>9</sup> Across jurisdictions, penalty structures systematically capture American firms. The EU extracted \$6.7 billion from U.S. tech companies in 2024 alone.<sup>10</sup>

DSTs represent direct revenue grabs. Unlike corporate income taxes on profits, DSTs tax gross revenue, sometimes with thresholds designed to capture only the largest platforms based on global income. France, the United Kingdom, Italy, Spain, Austria, and Turkey have implemented similar schemes, generating billions annually from American firms.<sup>11</sup>

Forced infrastructure investments constitute indirect extraction. Data localization mandates require American cloud providers to build local data centers simply to access markets. Network usage fees in South Korea force U.S. streaming platforms to pay Internet service providers (ISPs) mandatory charges that drive bandwidth costs to eight times those in Paris.<sup>12</sup> These are compelled capital transfers rather than routine compliance costs.

Proprietary asset disclosure forces the sharing of competitive advantages. Many interoperability mandates targeting American tech companies require platforms to expose application programming interfaces (APIs) and technical documentation to competitors.<sup>13</sup> Algorithm transparency rules compel disclosure of ranking systems and recommendation methods.

## **The Targeting Pattern**

These measures are engineered through policy design rather than explicit country-of-origin-based bans. Thresholds and definitions are set so that a small set of firms—primarily American—are captured, while domestic competitors are excluded from the scope.

Threshold engineering captures specific firms. DSTs with high global revenue triggers (e.g., €750 million+) predictably capture major U.S. platforms while excluding smaller local firms. The EU’s DMA gatekeeper criteria—€7.5 billion (\$8.72 billion) in annual European Economic Area (EEA) turnover, €75 billion (\$87 billion) in average market capitalization, and more than 45 million monthly active end users in the EU—were reverse-engineered to designate Apple, Google, Amazon, Meta, and Microsoft.<sup>14</sup> Indeed, DMA rapporteur Andreas Schwab stated openly that the regulation should focus on the five largest firms and not start with seven to include a European gatekeeper just to please the United States.<sup>15</sup>

GDPR enforcement demonstrates a discriminatory pattern: 9 of the 10 largest fines have been imposed on American companies, despite U.S. firms representing only 10 percent of EU information and communications technology (ICT) service imports.<sup>16</sup> As of April 2025, U.S. companies had paid €4.68 billion (\$5.44 billion) of the €5.65 billion (\$6.57 billion) in total GDPR fines—83 percent of the total.<sup>17</sup>

## **Offensive Strategy**

NTAs do more than restrict market access; they degrade competitive advantages and extract proprietary assets. These measures are not about building domestic capacity, but rather are structured to chip away at the advantages of a few specific, successful American firms by draining cash, eroding scale economies, and constraining product evolution.

Not all digital regulations are problematic. The concern lies with, for example, targeted ex ante regimes that preemptively redesign how a few platforms must operate without specific harm findings, and with extreme content rules that require 24-hour takedowns, strict liability, or broad risk-assessment duties that are hard to meet at scale. In practice, these approaches lead to unbundling and “equal-effectiveness” interoperability, force disclosure of technical documentation, mandate design and feature changes, and introduce turnover-based fines and network charges—mechanisms that, together, diminish the core differentiation users value in the market and transfer value to competitors or domestic intermediaries. Data-localization and “sovereign cloud” requirements trap capital in duplicated infrastructure and limit where and how firms can deploy computing resources, gradually weakening competitiveness over time.

Traditional protectionism is already disfavored under World Trade Organization (WTO) disciplines.<sup>18</sup> NTAs go beyond traditional protectionism and operate within the market. They are framed as privacy, competition, or consumer-protection measures. Yet, their design and application yield firm-specific outcomes: they impose structural handicaps on targeted companies while domestic competitors largely avoid comparable burdens. The result is not the nurturing of viable local alternatives, but rather the deliberate weakening of current leaders.

This systematic pattern—revenue extraction, precision targeting, competitive undermining, and strategic exclusion—reveals these measures as coordinated attacks on American technology leadership rather than legitimate regulatory responses to market failures.

## THE COST OF ATTACKS ON U.S. TECH

NTAs impose cascading costs that extend far beyond direct financial penalties. These measures systematically erode American technological leadership, weaken geopolitical influence, and extract hundreds of billions from the U.S. technology sector.

### Cost for the United States

#### Technology Leadership

##### Innovation Erosion Due to Diverted R&D and Regulatory Uncertainty

EU digital regulations depress market growth rates: Immediate revenue losses of \$33 billion in 2024 from advertising and platform restrictions have compounded over time as growth rates have slowed from a potential 28 percent to an actual 15.5 percent annually.<sup>19</sup> The accumulated revenue loss from EU digital regulations could reach \$2.2 trillion by 2030 across the five largest U.S. technology companies, translating into \$325 billion in foregone R&D investment.<sup>20</sup> This accounts for more than one-third of total U.S. annual R&D expenditures.<sup>21</sup> Regulatory uncertainty compounds these losses: Microsoft's six-month delay in launching Copilot in Europe due to compliance concerns under the DMA, the GDPR, and the AI Act cost the company \$2.3 billion in first-year revenue and reduced return on investment by 17.9 percentage points.<sup>22</sup>

This diversion of resources undermines America's ability to maintain its technological edge in critical emerging technologies such as AI, quantum computing, and advanced biotechnology, sectors where R&D leadership directly translates to economic and national security advantages.

##### Strategic Technology Losses Due to Mandatory Disclosure of Proprietary Systems or Forced Interoperability Mandates

The DMA's interoperability requirements force platforms to expose APIs and technical documentation to competitors, effectively transferring competitive advantages developed over years of R&D.<sup>23</sup> These mandates require companies to open tightly integrated ecosystems, weakening security architectures and enabling competitors to replicate proprietary features without the comparable investment.<sup>24</sup> Algorithm transparency rules compel disclosure of ranking systems and recommendation methods that constitute core intellectual property.<sup>25</sup>

These forced disclosures effectively subsidize foreign competitors' R&D by providing them with innovations that take American companies years and billions of dollars to develop, accelerating the erosion of U.S. competitive advantages.

##### Reduced Capital Investments Into Startups, Including Blocked Exit Strategies

Antitrust over-enforcement has created a "merger tax" that has reduced acquisitions of smaller startups by more than 95 percent.<sup>26</sup> This regulatory posture has constrained venture capital returns, increased startup shutdowns, and eliminated critical exit pathways for entrepreneurs.<sup>27</sup> This phenomenon is seen in the U.S. market too. FTC's blocking of Amazon's acquisition of iRobot exemplifies this dynamic: the company subsequently laid off workers and declined in value while Chinese competitors in robotic vacuum cleaners benefited from reduced competition.<sup>28</sup>



## Geopolitical Influence

### Gap Left by U.S. Companies Being Filled by State-Backed Chinese Companies

In markets wherein American firms face operational constraints or exclusion, Chinese state-backed enterprises expand unchallenged.<sup>29</sup> China currently controls approximately 40 percent of global 5G infrastructure through Huawei and ZTE and actively exports this technology through the Digital Silk Road initiative.<sup>30</sup> The DMA designates only one Chinese service (ByteDance) as a gatekeeper, while capturing multiple services from each of the five largest U.S. companies, creating asymmetric regulatory burdens that advantage Chinese competitors in both Europe and other third-party markets.<sup>31</sup>

This asymmetric regulatory environment serves as an industrial policy that advantages Chinese competitors while constraining American firms, accelerating China's efforts to displace U.S. technological leadership and extend its geopolitical influence through digital infrastructure.

### Reduced U.S. Technology Influence in Global Markets

The EU regulatory model has triggered global proliferation: Australia, Brazil, India, Japan, South Korea, and the United Kingdom have proposed or enacted similar digital regulations targeting U.S. firms.<sup>32</sup> This regulatory contagion fragments global markets and increases compliance complexity, while Chinese firms operate under comparatively lenient domestic regulations and benefit from state support in international expansion.<sup>33</sup>

## Cost for the American Tech Industry

### Fines and Fees

#### Total Fines Imposed on U.S. Tech Companies

Enforcement by the European Union has extracted unprecedented sums from American technology companies.<sup>34</sup> In 2024 alone, EU fines against U.S. tech firms totaled \$6.7 billion, representing nearly 20 percent of the EU's total tariff revenue base.<sup>35</sup> The four highest fines ever imposed by EU bodies targeted U.S. companies, including Google's \$5.1 billion Android penalty in 2018.<sup>36</sup> Between 2020 and 2023, GDPR enforcement alone generated \$3.1 billion in fines against U.S. companies, with American firms paying 83 percent of total GDPR penalties despite representing only 10 percent of EU ICT service imports.<sup>37</sup> These extraordinary fines function as discriminatory revenue extraction that disproportionately targets U.S. firms while generating billions for foreign treasuries.

---

**In 2024 alone, EU fines against U.S. tech firms totaled \$6.7 billion, representing nearly 20 percent of the EU's total tariff revenue base.**

---

## Compliance Burden

### Infrastructure Investment Requirements

Data localization mandates force U.S. companies to duplicate infrastructure across jurisdictions, increasing data hosting costs by 30 to 60 percent.<sup>38</sup> Building a major data center requires \$350 million to \$800 million in capital investment.<sup>39</sup> Mastercard's compliance with Indian localization requirements consumed \$350 million of its \$1 billion total investment in the country.<sup>40</sup> South Korea's network usage fees force U.S. streaming platforms to pay ISPs' mandatory charges that drive bandwidth costs to eight times those in Paris.<sup>41</sup> These duplicative requirements fragment



global cloud architectures and eliminate scale efficiencies that make American cloud services most competitive.

### **Estimated Legal and Compliance Costs**

Direct compliance costs for EU digital regulations total \$2.2 billion annually across the five largest U.S. technology companies.<sup>42</sup> DMA compliance alone requires \$200 million per year for each designated company.<sup>43</sup> The regulatory framework's complexity and ambiguity create additional financial risk exposure ranging from \$4.3 billion to \$12.5 billion per company annually, equivalent to an effective tax rate of 1.2 to 3.5 percent of global turnover.<sup>44</sup> DSTs in Austria, France, Italy, and Spain extracted an additional \$1.5 billion in 2023 alone, functioning as revenue-based tariffs that tax gross receipts rather than profits.<sup>45</sup>

### **Administrative Overhead Costs**

Meta had dedicated 590,000 engineering hours to DMA compliance by early 2024—equivalent to 355 full-time employees focused solely on regulatory adherence.<sup>46</sup> External compliance costs, including legal counsel, contractors, and audit services, add \$64 million annually per company under the DMA.<sup>47</sup> This “continuous defensive strategy” diverts executive management away from business strategy and product development, transforming innovation-focused organizations into compliance-centered operations.<sup>48</sup>

### **Forced Business Model Modifications**

The DMA mandates fundamental changes to core business practices: restrictions on data combination eliminate efficient advertising models; requirements for explicit user consent reduce conversion rates; and forced unbundling of integrated services degrades user experience.<sup>49</sup> These modifications are designed to “cut deep into the business models” of targeted companies. Platform openness requirements alone could generate \$8.2 billion to \$18.1 billion in lost revenue annually through mandated access grants to competitors.<sup>50</sup>

## **Opportunity Cost**

### **Lost Profits From Market Exclusions**

EU restrictions on data combination and advertising efficiency cost U.S. technology firms \$7.0 billion to \$14.8 billion in lost advertisement revenue in 2024 alone.<sup>51</sup> Forced business model changes and mandated openness to rivals resulted in additional losses of \$8.2 billion to \$18.1 billion in platform, subscription, and cloud revenues.<sup>52</sup> Product launch delays and market withdrawals compound such losses, causing companies to increasingly bypass European markets entirely rather than navigate regulatory uncertainty.

### **Foregone Growth Opportunities**

The cumulative impact of regulatory constraints creates compounding losses over time. By 2030, total accumulated revenue losses from EU digital regulation could range from \$879 billion to \$2.2 trillion across the five largest U.S. technology companies.<sup>53</sup> This foregone revenue would otherwise fund transformative R&D investments, next-generation infrastructure, and breakthrough innovations. Instead, these resources are diverted to compliance, fines, and defensive legal strategies, fundamentally altering the trajectory of American technological advancement.

## POLICY RECOMMENDATIONS

This section lists 11 recommendations, organized in 3 categories: identify and assess, engage and negotiate with leverage, and counter and deter.

### Identify and Assess

#### Consider National Competitiveness in Antitrust

##### Status Quo

U.S. antitrust enforcement operates under a consumer welfare standard that has proven flexible enough to address various competitive harms but lacks formal mechanisms to consider international competitiveness implications. DOJ's Antitrust Division and FTC make enforcement decisions independently, without structured input from DOC or other executive agencies on trade or national security effects. While the Committee on Foreign Investment in the United States reviews certain transactions for national security concerns, the antitrust agencies have no systematic process to weigh whether enforcement actions against U.S. firms might strengthen foreign competitors or harm U.S. strategic interests. And overall, historically, they have been indifferent to these impacts.<sup>54</sup> At the same time, they do not see it as within their scope to push back against their foreign counterparts when those counterparts use antitrust for competitive reasons.

---

**Foreign governments now cite U.S. antitrust enforcement as validation for discriminatory measures against American firms.**

---

##### Problem

This siloed, oblivious approach has contributed to the weakening of U.S. strategic industries. Sixty years of aggressive antitrust enforcement against Western Electric and AT&T systematically dismantled America's telecommunications equipment industry while other nations protected their champions, leaving the United States with no domestically owned telecom equipment companies today.<sup>55</sup> Foreign governments now exploit U.S. antitrust enforcement as validation for discriminatory measures against American firms. The problem extends globally: Google alone faces approximately 100 antitrust investigations worldwide, while the EU has levied over \$10 billion in antitrust fines against U.S. tech companies since 2017.<sup>56</sup> Foreign governments exploit U.S. antitrust actions to validate their own discriminatory measures—the EU explicitly cites U.S. cases to justify DMA provisions targeting American firms, creating a “Brussels effect” as similar laws spread to Brazil, India, Japan, and beyond.<sup>57</sup> Ironically, USTR lists these same foreign regulations as discriminatory trade barriers, yet DOJ and FTC enforcement provide political cover for them.<sup>58</sup> This creates a vicious cycle in which U.S. enforcement weakens American firms while foreign competitors receive state support and protected home markets. And U.S. antitrust officials give too much professional deference to their foreign counterparts, unwilling to acknowledge that they are increasingly using antitrust as an NTA.

##### Solution

The White House should direct DOJ and FTC to incorporate international competitiveness considerations into their prosecutorial discretion and remedy design after liability is established in cases involving strategic sectors, while also charging them with challenging foreign antitrust weaponization. For merger reviews, agencies should exercise prosecutorial discretion by not

spending scarce resources challenging deals with strong competitiveness justifications and instead prioritizing anticompetitive deals that lack such benefits. There is precedent from the 1950s, when the Pentagon successfully intervened in the AT&T case on national security grounds.<sup>59</sup> DOJ and FTC should be able to receive input on the competitiveness implications from relevant executive branch offices, including the Pentagon, DOC, and National Security Council, when finalizing remedies that could have international competitive effects.<sup>60</sup>

For conduct cases, the same principle applies: agencies should focus resources on cases without competitiveness concerns. In both merger reviews and conduct cases, while competitiveness considerations never determine whether conduct violates antitrust law, they should inform which cases merit limited enforcement resources and how remedies are designed after liability is established. DOJ and FTC should establish a formal consultation process whereby relevant executive branch agencies, including DOC and the National Security Council, provide input on international competitive effects before finalizing enforcement actions in strategic industries. The Trump administration should also direct DOJ and FTC to take a more active role in pushing back against foreign antitrust attacks on U.S. firms, including by filing formal submissions in foreign proceedings, issuing statements challenging discriminatory enforcement, and working through groups such as the International Competition Network and potentially the WTO to address these issues. This approach would maintain the consumer welfare standard's analytical rigor while ensuring that enforcement decisions account for national strategic interests, including effects on U.S. innovation capabilities and strategic industry leadership.

---

**The Trump Administration should direct DOJ and FTC to incorporate international competitiveness considerations into their prosecutorial discretion and remedial decisions in cases involving strategic sectors.**

---

## Require Periodic Economic Impact Assessments of NTAs

### Status Quo

USTR monitors compliance through the National Trade Estimate Report, which provides descriptive coverage but limited quantitative estimates of digital NTAs. USTR has been asked to enhance this reporting but lacks a standing, methodical framework to estimate the economic impact of digital NTAs on U.S. firms and the broader economy. No federal entity regularly estimates cumulative impacts on gross domestic product (GDP), export revenues, or R&D diversion stemming from discriminatory digital measures.

### Problem

Without measurement, NTAs proliferate unchecked. EU regulatory fines against U.S. tech firms totaled \$6.7 billion in 2024, yet broader economic impacts, such as compliance costs and ripple effects on the industry as a whole, remain unquantified.<sup>61</sup> Absent systematic data on economic losses and tax base erosion, policymakers cannot prioritize enforcement or demonstrate to trading partners the actual economic costs of their policies.

### Solution

Congress should direct USTR to enhance the National Trade Estimate Report with a dedicated section on digital NTBs and attacks, supported by DOC and the United States International Trade Commission. This enhanced section will map measures country by country, identify affected

sectors and firms, and provide clear cost bands for (a) fines and fees, (b) compliance and localization spending, and (c) mandated product or design changes, drawing on established international restrictiveness indicators and nontariff-measure datasets.<sup>62</sup>

A public, quarterly dashboard listing newly imposed and resolved measures by country, legal authority, and sector, with estimated cost bands and short notes on enforcement status, modeled on existing official barrier registries should be published.<sup>63</sup> For major actions, USTR should add a brief before-and-after check around the announcement or enforcement date and a two-page case note on observed impacts (an approach already used in trade policy studies).<sup>64</sup> Implementation would use the existing Trade Policy Staff Committee process: USTR coordinates inputs, DOC provides sector analysis (and can field a short annual survey of small and mid-size exporters), and the United States International Trade Commission conducts independent fact-finding.<sup>65</sup> This dashboard must explicitly flag countries that have trade agreements with the United States but are introducing domestic regulations that conflict with those agreements. It should list measures by country, legal authority, and sector.

---

**Absent systematic data on economic losses and tax base erosion, policymakers cannot prioritize enforcement or demonstrate to trading partners the actual economic costs of their policies.**

---

## Document Impact on SMEs and Innovation Ecosystem

### Status Quo

The U.S. government currently lacks a consistent mechanism to track and measure the impact of NTAs on American SMEs and the broader innovation ecosystem. While federal agencies monitor traditional trade barriers, there is no instrument to document how DSTs, localization, and design mandates affect SMEs' compliance burdens, export decisions, and access to platforms.<sup>66</sup> USTR's National Trade Estimate Report addresses certain NTBs but does not systematically capture their downstream effects on the innovation pipeline.

### Problem

This gap in documentation hides the full impact of NTAs on the U.S. economy. SMEs suffer disproportionately from NTBs because they lack the resources, management skills, and legal infrastructure to handle complex regulatory requirements across multiple jurisdictions.<sup>67</sup> When the EU imposes regulations with compliance costs that can reach billions of dollars, or when countries mandate data localization, smaller firms cannot absorb these costs as easily as large corporations can.<sup>68</sup> The damage extends beyond individual companies—NTAs “devastate U.S. small and medium enterprises that depend on these platforms while blocking crucial exit strategies for startups that rely on acquisitions to return capital to investors and fuel the next generation of innovation.”<sup>69</sup> This particularly threatens America's venture capital ecosystem, wherein SMEs and startups annually generate patents that are cited 8.5 percent more than established firms' patents are, demonstrating their outsized contribution to disruptive innovation.<sup>70</sup>

### Solution

The administration should incorporate digital non-tariff measures into existing firm-level surveys administered by the Commerce Department's International Trade Administration and the U.S. Small Business Administration. By adding NTA-specific modules to established surveys of

startups, SMEs, and digitally reliant firms, the government can capture compliance costs, market restrictions, and foregone opportunities without creating redundant data collection infrastructure. If necessary, the surveys would be expanded to include startups, SME manufacturers, and digital service providers to measure compliance costs, market restrictions, and missed opportunities due to discriminatory rules.<sup>71</sup> The assessment should track metrics such as regulatory compliance costs as a percentage of revenue for firms under \$100 million, startup formation rates in sectors affected by foreign regulations, venture capital trends after NTA changes, and disruptions in tech acquisitions.<sup>72</sup> This data would strengthen U.S. negotiations by providing concrete evidence of economic harm, supporting affected SMEs, and prioritizing specific NTAs to challenge through trade enforcement mechanisms.<sup>73</sup>

## Engage and Negotiate With Leverage

### Make Digital Barrier Removal a Priority in All Trade Negotiations

#### Status Quo

The Trump administration has elevated digital trade barriers as a negotiating priority, leveraging tariff threats to pressure countries such as Canada to abandon discriminatory DSTs. However, concrete outcomes have been limited. Despite these efforts, digital provisions can remain secondary to traditional trade concerns. While the United States-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement set high standards, most bilateral deals lack comprehensive digital provisions.<sup>74</sup> Despite trade agreements and commitments, countries continue pursuing discriminatory policies—South Korea, for example, is pushing DMA-style legislation that would grant its Fair Trade Commission broad discretion to target U.S. companies with arbitrary thresholds, even after committing in November 2025 to ensuring that U.S. companies “are not discriminated against.”<sup>75</sup> Trade negotiators prioritize traditional sectors such as agriculture and manufacturing, treating digital commerce as supplementary, even though over 50 percent of traded services depend on digital technologies.<sup>76</sup> The Biden administration’s withdrawal from the WTO Joint Statement Initiative on E-Commerce negotiations in 2023 ceded U.S. leadership as 49 other countries continued negotiations.<sup>77</sup>

#### Problem

This fragmented approach allows foreign governments to systematically target U.S. technology companies through NTAs—discriminatory regulations, forced data localization, and DSTs—while seeking access to American markets for their traditional goods.<sup>78</sup> The EU runs a trade surplus of over \$200 billion with the United States while imposing digital regulations that function as trade barriers against American firms.<sup>79</sup> China fills the vacuum left by U.S. companies’ retreat from markets due to discriminatory policies.<sup>80</sup> Without equal prioritization, American technology leadership erodes precisely when strategic competition intensifies.

#### Solution

The Trump administration should continue and expand efforts to make digital barrier removal a priority, through four steps:

1. Require binding commitments against discriminatory digital regulations with identical enforcement mechanisms to those for traditional trade violations.
2. Link enforcement across sectors—no agricultural or manufacturing concessions without reciprocal digital openness.

3. Standardize high-ambition digital chapters (e.g., USMCA-plus), adding AI-relevant provisions (e.g., data flows, narrow exceptions, algorithm/source-code protections with court-supervised access).<sup>81</sup>
4. Promote bilateral Digital Trade Agreements instead of trade deals without much weight.
5. Make carrying out commitments to roll back NTAs a condition for receiving a specific trade deal, including tariffs levels, from the president.

In addition, the Trump administration should enforce quarterly compliance reviews. Trade agreements cannot be “set it and forget it.” The administration should verify that partners are honoring their commitments. If the quarterly review identifies regression—such as a treaty partner adopting a discriminatory “digital sovereignty” law—the U.S. must immediately “revisit” the agreement in the subsequent quarter. This means pausing benefits or suspending cooperation until the regression is reversed. Given the administration’s three-year tariff policy horizon, these regular checkpoints create the necessary cadence to ensure that market access remains open.

This approach creates negotiating leverage that is currently absent when digital issues stand alone, reduces compliance costs resulting from regulatory fragmentation, and preserves U.S. competitive advantage in digital services. Implementation requires quarterly review and USTR coordination with Commerce and the State Department to ensure consistent enforcement across agreements.<sup>82</sup>

## Leverage AI Investments and Partnerships as Systemic Incentives

### Status Quo

The United States currently dominates global AI infrastructure, with American cloud providers controlling two-thirds of global cloud infrastructure and establishing technical standards through market adoption.<sup>83</sup> Countries worldwide now scramble to build “sovereign AI” capabilities by either developing domestic AI models or acquiring computing infrastructure.<sup>84</sup> Countries including the UAE, Saudi Arabia, Turkey, and nations across Africa and Latin America are actively courting American tech companies for AI partnerships, data centers, and cloud infrastructure investments. AI infrastructure has become a lever of national power; control over chips, cloud platforms, and data centers now shapes geopolitics.<sup>85</sup>

---

**U.S.-backed AI partnerships, infrastructure, and technology cooperation should be tied to verifiable commitments to open, nondiscriminatory digital and technology policies.**

---

### The Problem

The current approach underutilizes the United States’ position of dominating global AI infrastructure as a form of statecraft. Many governments seek U.S. AI investment while adopting discriminatory digital regulations modeled after European frameworks—data localization, selective enforcement, extractive fines, and design mandates—that weaken U.S. technology leadership precisely when scale advantages matter most against China’s state-directed model.<sup>86</sup> The fragmented approach allows countries to benefit from U.S. AI investments while maintaining protectionist policies, creating a situation in which American innovation subsidizes foreign digital sovereignty efforts without reciprocal market access.



## **Solution**

U.S.-backed AI partnerships, infrastructure, and technology cooperation should be tied to verifiable commitments to open, nondiscriminatory digital and technology policies. Partners that protect cross-border data flows, avoid forced localization, and enforce regulations transparently should receive deeper cooperation—access to advanced compute, cloud regions, and joint research—while partners that adopt or enforce discriminatory measures should face scaled-back cooperation or even suspension. Framed this way, countries face a straightforward choice: sustain discriminatory policies and limit access to U.S. AI capabilities or open their digital markets and fully participate in the U.S.-led AI ecosystem.<sup>87</sup>

## **Prioritize Digital Policy in Development Finance Corporation Investments**

### **Status Quo**

DFC currently provides \$9.3 billion annually in financing across developing countries without systematically conditioning investments on recipients' digital regulatory practices.<sup>88</sup> Most DFC-eligible markets maintain discriminatory digital policies—such as data localization requirements and DSTs targeting U.S. technology companies—yet DFC does not systematically consider these policies in investment decisions. Information Technology and Innovation Foundation (ITIF) research finds that DFC supports projects in countries on the USTR 301 Watch List and those engaging in digital trade restrictions.<sup>89</sup>

---

**DFC should prioritize investments in countries that demonstrate a commitment to nondiscriminatory digital policies, with particular attention to data centers, cloud infrastructure, and connectivity projects in which digital policy alignment matters most.**

---

### **Problem**

This unconditional approach undermines U.S. economic competitiveness by inadvertently subsidizing countries that actively harm American technology companies through NTAs. Countries receive U.S. development financing while simultaneously implementing policies that extract revenue from U.S. firms through discriminatory fines, data localization requirements, or regulatory barriers that favor domestic competitors. This creates a perverse incentive structure wherein developing nations can benefit from U.S. largesse while undermining U.S. commercial interests. The absence of conditionality also represents a missed opportunity to leverage DFC's considerable financial resources—approaching its \$60 billion exposure cap—to incentivize market-friendly digital policies before protectionist measures become entrenched.<sup>90</sup>

### **Solution**

DFC should prioritize investments in countries that demonstrate a commitment to nondiscriminatory digital policies, with particular attention to data centers, cloud infrastructure, and connectivity projects in which digital policy alignment matters most. DFC should develop a digital policy scorecard to assess recipient countries' regulatory environments as one factor in investment decisions, alongside national security, development impact, and other strategic priorities. This approach would signal U.S. preferences for open digital markets while maintaining flexibility to pursue investments that serve broader strategic objectives. DFC could emphasize digital policy openness in regions where China's Digital Silk Road offers alternative financing, demonstrating that U.S. partnership supports both development goals and market-oriented digital policies.<sup>91</sup>



## Restore and Expand Digital Policy Capacity Building for Developing Countries

### Status Quo

The State Department's Bureau of Cyberspace and Digital Policy was established to advance U.S. digital policy interests globally and maintains digital attachés in 16 markets, but the bureau has been significantly reduced in recent years, limiting its capacity for systematic engagement.<sup>92</sup> Technical assistance on digital regulation remains fragmented across agencies, and there is no coordinated messaging on market-friendly strategies. Many developing countries gain their primary understanding of digital regulatory models from EU officials promoting restrictive frameworks or Chinese representatives pushing authoritarian approaches.

### Problem

Developing nations often adopt harmful digital policies not out of protectionist intent but because they lack awareness of their negative impacts on their economies.<sup>93</sup> Without sustained U.S. engagement, developing country policymakers often turn to EU officials advocating the DMA or Chinese representatives promoting digital sovereignty, adopting these models despite their economic costs. The EU exports its regulatory framework through technical assistance, framing discriminatory policies as “global best practices.” This regulatory influence harms U.S. interests and developing countries, as studies show that they would lose more GDP than gain in digital protectionism revenue.<sup>94</sup> The U.S. approach is too limited to counter these influence campaigns effectively.

### Solution

Congress should restore funding and expand the mandate of the State Department's Bureau of Cyberspace and Digital Policy, specifically establishing a dedicated Office of International Digital Policy Engagement and Capacity Building within the bureau to consolidate technical assistance efforts. This office would expand the digital attaché program to 50+ priority markets, facilitate dialogue with developing country policymakers on digital regulatory approaches, and provide technical assistance on how open digital policies can boost economic growth while addressing legitimate policy concerns. Programs would include collaborative economic analysis with developing countries, showing how various regulatory approaches affect foreign investments, technology transfers, and domestic digital businesses. Partnerships with U.S. tech companies would offer case studies and expertise. Focus should be on countries considering DSTs or data localization, engaging in dialogue about alternative revenue models and data frameworks that protect national sovereignty while maintaining digital market openness. The office would coordinate with Commerce and other agencies participating in the Digital Connectivity and Cybersecurity Partnership to ensure consistent U.S. engagement on digital policy.<sup>95</sup>

## Counter and Deter

### Prevent NTAs from Becoming Global Norms Through Multilateral Forums

#### Status Quo

The United States participates in multilateral organizations (OECD, G7, G20, UN, ITU) without a coordinated counterstrategy to address systematic efforts by the EU and China to legitimize their digital governance models as international standards. The EU explicitly aims to “assert its position with a leading voice” at these forums to embed its data protection principles in global rules.<sup>96</sup> China actively promotes “cyber sovereignty” through the World Internet Conference,

International Telecommunication Union (ITU), and UN forums, with a Chinese national heading the ITU since 2014.<sup>97</sup>

### **Problem**

The EU and China use multilateral forums to normalize discriminatory policies as “best practices”—the EU through regulatory frameworks, China through state-controlled governance models. The Brussels Effect has succeeded globally, with Argentina, Brazil, Japan, Nigeria, South Korea, Thailand, and Turkey adopting GDPR-inspired frameworks.<sup>98</sup> China advocates for ITU control over Internet architecture and “multilateral” state-based governance that challenges the multistakeholder model.<sup>99</sup> Once either framework gains multilateral endorsement, countries adopt them to appear compliant with emerging norms. This creates a two-front challenge: U.S. firms face discriminatory EU regulations and authoritarian Chinese controls being legitimized through institutions, while U.S. principles of open Internet governance lose ground. This process transforms bilateral trade disputes into multilateral consensus against U.S. interests, with American taxpayers effectively funding organizations that undermine U.S. competitiveness through their contributions to these institutions.

---

**U.S. firms face discriminatory EU regulations and authoritarian Chinese controls being legitimized through institutions, while U.S. principles of open Internet governance lose ground.**

---

### **Solution**

The Trump administration should significantly increase U.S. engagement in multilateral organizations to actively counter efforts to legitimize discriminatory digital policies, while reserving the option to condition funding in cases of systematic bias against U.S. economic interests. The State Department’s Bureau of Economic and Business Affairs should expand and strengthen existing multilateral digital policy programs with dedicated resources and clearer mandates to engage proactively in standard setting at international forums. U.S. foreign officials should systematically challenge discriminatory policies, build coalitions with like-minded countries, and propose alternative frameworks that protect legitimate policy interests without resorting to protectionist trade barriers or attacks. The United States should complement multilateral engagement with bilateral and plurilateral initiatives, such as the Digital Connectivity and Cybersecurity Partnership, that promote open digital markets and demonstrate viable alternatives to protectionist frameworks. Congress should require annual reports assessing how multilateral organizations’ digital policy positions affect U.S. economic interests, with authority to adjust U.S. funding levels for organizations that systematically promote discriminatory policies despite U.S. objections.<sup>100</sup> This strategy prevents protectionist policies from being legitimized through international institutions by ensuring robust U.S. engagement and leadership in multilateral forums, while maintaining accountability for U.S. taxpayer contributions.

## **Launch Section 301 Investigations Into Major NTAs**

### **Status Quo**

Section 301 of the Trade Act of 1974 provides USTR with authority to investigate and respond to unfair trade practices, but its application remains largely oriented toward traditional trade in goods through tariff mechanisms. The administration has initiated investigations into digital service taxes and certain digital sovereignty initiatives, but these investigations remain limited in scope, and enforcement tools are outdated for the digital economy.<sup>101</sup>

## Problem

The EU's DMA and DSA exemplify the most egregious targeting of U.S. technology firms through discriminatory regulation that affects American competitiveness and innovation. The DMA's revenue and market capitalization thresholds—€7.5 billion in annual EEA turnover or €75 billion market cap—were explicitly designed to capture U.S. tech giants while exempting most European competitors, as DMA rapporteur Andreas Schwab advocated.<sup>102</sup> These regulations stifle innovation, create compliance burdens estimated in billions of dollars annually, and provide a protectionist model for other countries to emulate. Beyond the DMA and DSA, the EU's discriminatory enforcement of GDPR, extractive fines, and digital sovereignty initiatives collectively undermine U.S. technological leadership and extract revenue from American companies to subsidize European competitors.<sup>103</sup>

## Solution

Congress should amend Section 301 to detail specific mechanisms and processes for imposing retaliatory measures on foreign service providers, including licensing requirements, certification restrictions, and reciprocal joint venture mandates.<sup>104</sup> The administration should launch comprehensive Section 301 investigations into the EU's DMA, DSA, and discriminatory GDPR enforcement patterns, documenting anticompetitive distortions with detailed economic assessments. These investigations should expand beyond DSTs to encompass the full spectrum of digital discrimination, including cybersecurity regulations and cloud sovereignty requirements. The administration could implement retaliation through traditional tariffs, taxes, or restrictions on EU digital service companies operating in the United States, as well as limitations on other EU service providers, including accounting firms, air carriers, and media companies.<sup>105</sup> This approach would establish credible deterrence while maintaining flexibility for negotiated settlements that address the underlying discriminatory practices.

---

**The administration should launch comprehensive Section 301 investigations into the EU's DMA, DSA, and discriminatory GDPR enforcement patterns, documenting anticompetitive distortions with detailed economic assessments.**

---

## Re-engage in Multilateral Digital Trade/Digital Economy Disciplines Outside the WTO

### Status Quo

The United States withdrew from digital trade commitments at the WTO in 2023 and has retreated from leadership in establishing binding digital trade rules, creating a vacuum filled by China's digital sovereignty model and European regulatory imperialism. The CPTPP contains advanced digital trade provisions, including prohibitions on data localization, protection of cross-border data flows, and nondiscrimination for digital products, but the United States remains outside this framework.<sup>106</sup>

### Problem

U.S. withdrawal from multilateral digital trade negotiations undermines American technological leadership and allows adversaries to shape global digital governance. China exploits the absence of U.S. leadership to advocate for broad national security exceptions that justify data localization, while the EU exports its regulatory model globally.<sup>107</sup> Without binding international commitments, U.S. firms face an increasingly fragmented global digital economy with conflicting requirements across jurisdictions. The absence of dispute-resolution mechanisms for digital trade

leaves American companies vulnerable to discriminatory treatment with no recourse. Countries such as India leverage “policy space” arguments to justify protectionist measures, citing U.S. withdrawal as validation for data sovereignty approaches.<sup>108</sup>

### **Solution**

The United States should join the CPTPP, which already includes key allies such as Japan, Canada, and Australia. The CPTPP was conceived to counter China’s growing influence in the Asia-Pacific region; the United States should resume its role in this initiative. The condition for joining the agreement must include binding commitments to ensure cross-border data flows for business purposes, with only narrow, necessary exceptions for legitimate public policy objectives that do not constitute disguised protectionism.<sup>109</sup> This framework creates a competitive advantage for open, rules-based digital economies by enabling trusted digital partnerships among countries with compatible governance systems, providing a clear alternative to authoritarian digital governance models that rely on state surveillance and discriminatory enforcement.

---

**Diplomatic protests without credible enforcement fail to deter discriminatory practices against U.S. technology firms, as evidenced by the EU’s continued escalation of protectionist digital sovereignty measures despite years of U.S. concerns.**

---

## **Implement Reciprocal Measures With Escalating Consequences**

### **Status Quo**

The United States has primarily relied on diplomatic complaints and dialogue to address digital protectionism, with limited use of trade enforcement tools that almost always fail to change foreign behavior. The fact that the Biden administration’s Trade and Technology Council explicitly excluded NTAs from the dialogue is a case in point. The Trump administration has increased its use of trade retaliatory measures, but these responses have lacked consistency. Meanwhile, countries that impose discriminatory measures against American tech companies continue to secure favorable trade agreements without any compromise to their digital policies. Current responses still lack clear escalation triggers, predictable consequences, or coordination across different policy tools, undermining deterrence.<sup>110</sup>

### **Problem**

Diplomatic protests without credible enforcement fail to deter discriminatory practices against U.S. technology firms, as evidenced by the EU’s continued escalation of protectionist digital sovereignty measures despite years of U.S. concerns. The absence of clear escalation thresholds enables foreign governments to incrementally increase protectionist measures without facing meaningful consequences. Uncoordinated responses across different U.S. agencies reduce effectiveness and allow targeted countries to exploit gaps. The EU maintains a \$200 billion trade surplus with the United States while systematically discriminating against American tech companies, demonstrating that current approaches lack leverage.<sup>111</sup>

### **Solution**

USTR, in coordination with the Commerce, Treasury, and State departments, should establish a structured escalation framework that begins with formal diplomatic warnings that specify precise concerns and required remedies within defined timeframes. Escalation decisions should be informed by rigorous economic analysis, quantifying the harm to U.S. firms and the broader

economy from discriminatory measures.<sup>112</sup> If initial consultations fail, targeted regulatory measures beyond traditional tariffs, such as using DOC ICT service reviews to scrutinize EU firms' transactions with foreign adversaries, implementing mirror taxes through Section 891 of the Internal Revenue Code to match discriminatory DSTs, and restricting federal procurement opportunities for firms from non-compliant countries, should be implemented.<sup>113</sup> The framework should define specific triggers for escalation based on quantified economic-harm thresholds, the number of affected U.S. companies, and evidence of systemic discrimination rather than isolated incidents, making use of the quarterly dashboard listing newly imposed and resolved measures by jurisdiction. If a country is flagged for regression or new NTAs and fails to "change course" within one quarterly review cycle, the United States should automatically consider proceeding to the next tier of consequences (i.e., from diplomatic warning to 301 investigation). This moves enforcement away from ad hoc political decisions and toward a predictable consequence structure based on quantified economic harm and systemic discrimination.

Credible deterrence must be maintained by demonstrating willingness to impose costs while preserving off-ramps for negotiated solutions that address core U.S. concerns. This approach would incentivize compliance by ensuring there are predictable consequences while avoiding unnecessary trade conflicts that harm both economies involved in any given dispute.

## About the Authors

Dr. Robert D. Atkinson (@RobAtkinsonITIF) is the founder and president of ITIF. His books include *Technology Fears and Scapegoats: 40 Myths About Privacy, Jobs, AI and Today's Innovation Economy* (Palgrave MacMillan, 2024); *Big Is Beautiful: Debunking the Myth of Small Business* (MIT, 2018); *Innovation Economics: The Race for Global Advantage* (Yale, 2012); *Supply-Side Follies: Why Conservative Economics Fails, Liberal Economics Falters, and Innovation Economics Is the Answer* (Rowman Littlefield, 2007); and *The Past and Future of America's Economy: Long Waves of Innovation That Power Cycles of Growth* (Edward Elgar, 2005). He holds a Ph.D. in city and regional planning from the University of North Carolina, Chapel Hill.

Hilal Aka was a policy analyst at ITIF focusing on U.S. technology competitiveness. Previously, she interned with the Center for a New American Security's technology and national security program and was an economic consultant on antitrust and competition matters at Charles River Associates. She holds a bachelor's degree from Wellesley College with a double major in economics and mathematics.

## About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit [itif.org/about](https://itif.org/about).

## ENDNOTES

---

1. Hilal Aka, “EU Regulatory Actions Against US Tech Companies Are a De Facto Tariff System” (ITIF, April 28, 2025), <https://itif.org/publications/2025/04/28/de-facto-eu-tariff-system/>.
2. Daniel Castro, “Europe’s GDPR Fines Against US Firms Are Unfair and Disproportionate” (Center for Data Innovation), April 2025, <https://datainnovation.org/2025/04/europes-gdpr-fines-against-us-firms-are-unfair-and-disproportionate/>.
3. Hilal Aka, “Defending US Technology Leadership From Nontariff Attacks” (ITIF, 2025), <https://www2.itif.org/2025-aka-nontariff-attacks.pdf>
4. European Commission, “Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service,” press release, June 27, 2017, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_17\\_1784](https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784); Court of Justice of the European Union, “Google loses final EU court appeal against 2.4 billion euro fine in antitrust shopping case,” press release, September 10, 2024; Inside Indiana Business, “Google data center investment in Fort Wayne grows to \$2 billion,” April 26, 2024, <https://www.insideindianabusiness.com/articles/google-data-center-project-in-fort-wayne-grows-to-2-billion>; Indiana Economic Development Corporation, “Gov. Holcomb announces Google is building a \$2B Data Center in Northeast Indiana,” press release, April 26, 2024.
5. Jane G. Gravelle, “The OECD/G20 Pillar 1 and Digital Services Taxes: A Comparison,” Congressional Research Service Report R47988 (2024), <https://crsreports.congress.gov/product/pdf/R/R47988>.
6. Lilla Nóra Kiss, “Does the DMA Intentionally Target US Companies?” (ITIF, May 2025), <https://itif.org/publications/2025/03/21/does-the-dma-intentionally-target-us-companies/>; Joseph V. Coniglio, and Lilla Nóra Kiss, “Comments to the European Commission for Its First Review of the Digital Markets Act” (ITIF, September 2025), <https://itif.org/publications/2025/09/24/comments-to-the-european-commission-for-its-first-review-of-the-digital-markets-act/>.
7. Hadi Houalla, “Turkey’s DMA Spinoff Is Another Threat to Global Innovation” (ITIF, February 26, 2024), <https://itif.org/publications/2024/02/26/turkeys-dma-spinoff-is-another-threat-to-global-innovation/>.
8. Norton Rose Fulbright, “India: Competition law fact sheet,” accessed October 28, 2025, <https://www.nortonrosefulbright.com/en/knowledge/publications/ba1b31d2/competition-law-fact-sheet-india>.
9. Anna Moskal and Marcella Brandão Flores da Cunha, “Brazil’s Path towards Digital Ex Ante Competition Regulation – Remarks on the Brazilian Ministry of Finance 2024 Proposal,” *Kluwer Competition Law Blog*, April 4, 2025, <https://competitionlawblog.kluwercompetitionlaw.com/2025/04/04/brazils-path-towards-digital-ex-ante-competition-regulation-remarks-on-the-brazilian-ministry-of-finance-2024-proposal/>.
10. Aka, “EU Regulatory Actions Against US Tech Companies Are a De Facto Tariff System.”
11. Tax Foundation, “Digital Services Taxes State of Play” (July 7, 2025), <https://taxfoundation.org/blog/digital-services-tax-us-trade/>.
12. Joe Kane and Jessica Dine, “Consumers Are the Ones Who End Up Paying for Sending-Party-Pays Mandates” (ITIF, November 7, 2022), <https://itif.org/publications/2022/11/07/consumers-are-the-ones-who-end-up-paying-for-sending-party-pays-mandates/>.
13. European Commission, “Interoperability - Digital Markets Act (DMA),” [https://digital-markets-act.ec.europa.eu/questions-and-answers/interoperability\\_en](https://digital-markets-act.ec.europa.eu/questions-and-answers/interoperability_en); “The EU’s Digital Markets Act: What Does It Mean for Businesses and Data Privacy?” Orrick, November 2022, <https://www.orrick.com/en/Insights/2022/11/The-EUs-Digital-Markets-Act-What-Does-It-Mean-for-Businesses-and-Data-Privacy>.



14. “Deal on Digital Markets Act: ensuring fair competition and more choice for users,” European Parliament, March 24, 2022, <https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users>.
15. Kiss, “Does the DMA Intentionally Target US Companies?”; Javier Espinoza, “EU should focus on top 5 tech companies, says leading MEP,” *Financial Times*, May 30, 2021, <https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b>.
16. Castro, “Europe’s GDPR Fines Against US Firms Are Unfair and Disproportionate.”
17. Ibid.
18. Gisela Grieger, “Understanding import tariffs under WTO law,” European Parliament Think Tank, March 21, 2025, <https://epthinktank.eu/2025/03/21/understanding-import-tariffs-under-wto-law/>; “General Agreement on Tariffs and Trade (GATT),” Britannica, accessed October 28, 2025, <https://www.britannica.com/topic/General-Agreement-on-Tariffs-and-Trade>.
19. The \$2.2 trillion figure represents cumulative projected revenue loss from 2024 to 2030, calculated by comparing two growth trajectories. The methodology: (1) In 2024, EU regulations directly reduced revenues by an estimated \$33 billion through restrictions on data usage for advertising (\$14.8 billion loss) and DMA requirements that depress platform/subscription/cloud services (\$18.1 billion loss). (2) These immediate losses reduced the annual growth rate of EU digital services revenues from a potential 28 percent (calculated by adding back the 10 percent foregone revenues to establish a counterfactual baseline consistent with less mature digital markets) to an actual 15.5 percent observed in 2023–2024. (3) This 12.5-percentage-point growth differential, when compounded over seven years (2024–2030), produces a cumulative gap of \$2.2 trillion between what revenues would have been without EU regulations versus projected actual revenues. Since the five largest U.S. technology companies invest approximately 15 percent of revenues in R&D, this translates to \$325 billion in foregone R&D investment. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation” (March 2025), [https://ccianet.org/wp-content/uploads/2025/03/CCIA\\_EU-Digital-Regulation-Factsheet\\_reportfinal.pdf](https://ccianet.org/wp-content/uploads/2025/03/CCIA_EU-Digital-Regulation-Factsheet_reportfinal.pdf).
20. Ibid.
21. Ibid.
22. Ibid.
23. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; “The US Cost of Europe’s Digital Markets Act,” American Enterprise Institute, October 15, 2025, <https://www.aei.org/technology-and-innovation/the-us-cost-of-europes-digital-markets-act/>.
24. “The US Cost of Europe’s Digital Markets Act.”
25. Ibid.; Robert D. Atkinson, “Testimony Before the U.S. House Ways and Means Committee Subcommittee on Trade: Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules” (September 20, 2024), [https://waysandmeans.house.gov/wp-content/uploads/2024/09/2024-atkinson-testimony-digital-trade\\_shortened.pdf](https://waysandmeans.house.gov/wp-content/uploads/2024/09/2024-atkinson-testimony-digital-trade_shortened.pdf).
26. Logan Kolas, “60 Minutes of Missed Opportunities,” The American Consumer Institute Center for Citizen Research, September 27, 2024, <https://www.theamericanconsumer.org/2024/09/60-minutes-of-missed-opportunities/>; “Restrictive M&A Threatens America’s AI Leadership Plan,” Springboard, November 12, 2025, <https://springboardccia.com/2025/11/12/restrictive-ma-threatens-americas-ai-leadership-plan/>; Sam Bowman and Sam Dumitriu, “Better Together: The Procompetitive Effects of Mergers in Tech” (The Entrepreneurs Network, October 1, 2021), <https://www.tenentrepreneurs.org/research/better-together-the-procompetitive-effects-of-mergers-in-tech>; Jonathan M. Barnett, “‘Killer Acquisitions’ Reexamined: Economic Hyperbole in the Age of



- Populist Antitrust,” University of Chicago Business Law Review, no. 3 (2024): 39, [https://businesslawreview.uchicago.edu/sites/default/files/2024-01/Barnett\\_0.pdf](https://businesslawreview.uchicago.edu/sites/default/files/2024-01/Barnett_0.pdf).
27. Kolas, “60 Minutes of Missed Opportunities”; “Restrictive M&A Threatens America’s AI Leadership Plan”; Bowman and Dumitriu, “Better Together: The Procompetitive Effects of Mergers in Tech.”
  28. “Wake-Up Call on U.S. Competitiveness Was Overdue,” Disruptive Competition Project, January 31, 2025, <https://project-disco.org/competition/wake-up-call-on-us-competitiveness-was-overdue/>.
  29. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; Matthias Bauer, Dyuti Pandya, and Vanika Sharma, “EU Export of Regulatory Overreach: The Case of the Digital Markets Act (DMA)” (ECIPE, 2025), <https://ecipe.org/publications/eu-export-of-regulatory-overreach-dma/>; Emily Wu, “Sovereignty and Data Localization” (Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2021), <https://www.belfercenter.org/publication/sovereignty-and-data-localization>.
  30. Wu, “Sovereignty and Data Localization.”
  31. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; Bauer, Pandya, and Sharma, “EU Export of Regulatory Overreach”; Wu, “Sovereignty and Data Localization.”
  32. Atkinson, “Testimony Before the U.S. House Ways and Means Committee”; Bauer, Pandya, and Sharma, “EU Export of Regulatory Overreach.”
  33. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; Bauer, Pandya, and Sharma, “EU Export of Regulatory Overreach”; Hodan Omaar, “AI Sovereignty Makes Everyone Weaker—America Can Lead Differently,” Center for Data Innovation, September 12, 2025, <https://datainnovation.org/2025/09/ai-sovereignty-makes-everyone-weaker-the-us-can-lead-differently/>; Ikechukwu Nwabufu and Daberechukwu Egbo, “Reevaluating American Antitrust Laws Towards Unlocking Manufacturing Competitiveness,” *International Journal of Research and Innovation in Social Science* 9, no. 4 (April 2025): 869–879, <https://rsisinternational.org/journals/ijriss/articles/reevaluating-american-antitrust-laws-towards-unlocking-manufacturing-competitiveness/>; Atkinson, “Testimony Before the U.S. House Ways and Means Committee.”
  34. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; Aka, “EU Regulatory Actions Against US Tech Companies Are a De Facto Tariff System.”
  35. Aka, “EU Regulatory Actions Against US Tech Companies.”
  36. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation.”
  37. Atkinson, “Testimony Before the U.S. House Ways and Means Committee.”
  38. Wayan Vota, “Data Localization Is a Political Decision, Not a Technological One,” ICTworks, <https://www.ictworks.org/data-localization-political-decision/>; Conan French, Brad Carr, and Clay Lowery, “Data Localization: Costs, Tradeoffs, and Impacts Across the Economy” (Institute of International Finance, December 2020), [https://www.iif.com/portals/0/Files/content/Innovation/12\\_22\\_2020\\_data\\_localization.pdf](https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf); Lindsey R. Sheppard, Erol Yayboke, and Carolina G. Ramos, “The Real National Security Concerns over Data Localization” (CSIS, August 2021), <https://www.csis.org/analysis/real-national-security-concerns-over-data-localization>; Wu, “Sovereignty and Data Localization.”
  39. Ibid.
  40. Wu, “Sovereignty and Data Localization.”
  41. Atkinson, “Testimony Before the U.S. House Ways and Means Committee.”

42. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation.”
43. Ibid.; “The US Cost of Europe’s Digital Markets Act.”
44. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation.”
45. Daniel Bunn, “Digital Services Taxes State of Play,” *Tax Foundation blog*, July 7, 2025, <https://taxfoundation.org/blog/digital-services-tax-us-trade/>.
46. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; Coniglio and Kiss, “Comments to the European Commission for Its First Review of the Digital Markets Act.”
47. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation.”
48. Ibid.
49. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation”; Coniglio and Kiss, “Comments to the European Commission.”
50. CCIA Research Center and LAMA Economic Research, “Costs to U.S. Companies from EU Digital Regulation.”
51. Ibid.
52. Ibid.
53. Ibid.
54. Robert D. Atkinson and David Moschella, “The Myth About ‘Hi-Tech’ Antitrust Success” (ITIF, October 17, 2023), <https://itif.org/publications/2023/10/17/the-myth-about-hi-tech-antitrust-success/>.
55. Robert D. Atkinson, “Who Lost Lucent?: The Decline of America’s Telecom Equipment Industry,” *American Affairs Journal*, August 20, 2020, <https://americanaffairsjournal.org/2020/08/who-lost-lucent-the-decline-of-americas-telecom-equipment-industry/>.
56. “EU tech rules should only target dominant companies, EU lawmaker says,” *Reuters*, June 1, 2021, <https://www.reuters.com/technology/eu-tech-rules-should-only-target-dominant-companies-eu-lawmaker-says-2021-06-01/>.
57. Christian Bergqvist, ProMarket website, February 19, 2024, <https://www.promarket.org/2024/02/19/taking-stock-of-googles-antitrust-troubles-as-the-world-turns-against-it/>; Ronan Murphy, “Mapping the Brussels Effect,” (CEPA, July 2025), <https://cepa.org/comprehensive-reports/the-brussels-effect-goes-global/>.
58. Office of the United States Trade Representative, “2024 National Trade Estimate Report on Foreign Trade Barriers,” March 2024, <https://ustr.gov/sites/default/files/2024-03/2024%20NTE%20Report.pdf>.
59. There are historical examples of competitiveness concerns informing the decision whether to bring cases—such as when Defense Secretary Charles Wilson successfully intervened in the 1950s AT&T case on national security grounds. Atkinson, “Who Lost Lucent?”
60. Atkinson, “Testimony Before the U.S. House Ways and Means Committee.”
61. Robert D. Atkinson et al., “Letter to the Trump Administration Regarding Non-Tariff Attacks” (ITIF, July 2, 2025), <https://itif.org/publications/2025/07/02/letter-regarding-non-tariff-attacks-on-us-tech-firms-and-industries/>.
62. United States International Trade Commission, “Understanding General Factfinding Investigations (Section 332),” [https://www.usitc.gov/press\\_room/general\\_factfinding.htm](https://www.usitc.gov/press_room/general_factfinding.htm); United States

- International Trade Commission, “Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions” (Publication 4716, August 2017), <https://www.usitc.gov/publications/332/pub4716.pdf>; United States International Trade Commission, Foreign Censorship, “Part 2: Trade and Economic Effects on U.S. Businesses” (Publication 5334, July 2022), <https://www.usitc.gov/publications/332/pub5334.pdf>; OECD, “Services Trade Restrictiveness Index,” <https://www.oecd.org/en/topics/sub-issues/services-trade-restrictiveness-index.html>; OECD, “Digital Services Trade Restrictiveness Index,” <https://goingdigital.oecd.org/en/indicator/73>; United Nations Conference on Trade and Development (UNCTAD), “TRAINS—Non-Tariff Measures Data,” <https://trainsonline.unctad.org/>; Jose Durán Lima et al., “Assessing the Impact of Non-Tariff Barriers during the Global Crisis: The Experience in Argentina, Ecuador and Venezuelans” (paper presented at the 13th Annual Conference on Global Economic Analysis, Penang, Malaysia, 2010), [https://www.gtap.agecon.purdue.edu/resources/res\\_display.asp?RecordID=3383](https://www.gtap.agecon.purdue.edu/resources/res_display.asp?RecordID=3383).
63. For example, Shanker A. Singham and Alden F. Abbott, *Trade, Competition and Domestic Regulatory Policy* (Routledge, 2023); Shanker A. Singham, *International Trade, Regulation and the Global Economy: The Impact of Anti-Competitive Market Distortions* (Routledge, 2025). The Anti-Competitive Market Distortions (ACMD) model provides a two-stage methodology for quantifying the economic impacts of regulatory measures that deviate from sound competition policy principles. The model estimates both direct costs to affected firms and broader GDP impacts, demonstrating that anticompetitive regulatory measures can impose costs three to four times larger than traditional border barriers. See Compete Foundation, “Anti-Competitive Market Distortions Model,” <https://www.competerefoundation.org/>; Department for Business and Trade (United Kingdom), “Market Access Barrier Statistics (collection),” <https://www.gov.uk/government/collections/market-access-barrier-statistics>; European Commission, “Access2Markets—Trade Barriers,” <https://trade.ec.europa.eu/access-to-markets/en/barriers>.
  64. United States International Trade Commission, “Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses” (Publication 5334, July 2022), <https://www.usitc.gov/publications/332/pub5334.pdf>.
  65. United States International Trade Commission, “Understanding General Factfinding Investigations (Section 332),” [https://www.usitc.gov/press\\_room/general\\_factfinding.htm](https://www.usitc.gov/press_room/general_factfinding.htm); United States International Trade Commission, “Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions” (Publication 4716, August 2017), <https://www.usitc.gov/publications/332/pub4716.pdf>; United States International Trade Commission, “Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses” (Publication 5334, July 2022), <https://www.usitc.gov/publications/332/pub5334.pdf>.
  66. Robert D. Atkinson, “Testimony to the US House Ways and Means Trade Subcommittee: Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules” (ITIF, September 2024), <https://itif.org/publications/2024/09/20/testimony-house-ways-and-means-trade-subcommittee-strong-digital-trade-rules/>.
  67. World Trade Organization, World Trade Report 2016: Levelling the Trading Field for SMEs (Geneva: WTO, 2016), [https://www.wto.org/english/res\\_e/booksp\\_e/wtr16-1\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/wtr16-1_e.pdf).
  68. Stephen Ezell and Stefan Koester, “Transforming Global Trade and Development With Digital Technologies” (ITIF, May 2023), <https://itif.org/publications/2023/05/08/transforming-global-trade-and-development-with-digital-technologies/>.
  69. Atkinson et al., “Letter to the Trump Administration Regarding Non-Tariff Attacks.”
  70. Miranda Fraraccio, “How Startups Contribute to Innovation in Emerging Industries,” U.S. Chamber of Commerce, April 15, 2024, <https://www.uschamber.com/co/start/strategy/startup-ingenuity-and->

- innovation, cited in Trelysa Long, “How Digital Services Empower SMEs and Start-Ups” (ITIF, August 2025), <https://itif.org/publications/2025/08/27/how-digital-services-empower-smes-and-start-ups/>.
71. Stephen Ezell, “Accelerating Digital Technology Adoption Among U.S. Small and Medium-Sized Manufacturers” (ITIF, April 2024), <https://itif.org/publications/2024/04/19/accelerating-digital-technology-adoption-among-smes/>.
  72. Robert D. Atkinson and Ian Tufts, “The Hamilton Index, 2023: China Is Running Away With Strategic Industries” (ITIF, December 2023), <https://itif.org/publications/2023/12/13/2023-hamilton-index/>.
  73. Hilal Aka, “Trade Talks Must Confront Foreign Non-Tariff Attacks on American Tech” (ITIF, April 2025), <https://itif.org/publications/2025/04/10/trade-confront-foreign-attacks-american-tech/>.
  74. ICT Services and Digital Trade,” Office of the United States Trade Representative, accessed October 27, 2025, <https://ustr.gov/issue-areas/services-investment/telecom-e-commerce>.
  75. Rodrigo Balbontin and Sejin Kim, “The Korean Government Should Keep Its Word and Push Against the Misleading ‘Fairness Act’” (ITIF, November 20, 2025), <https://itif.org/publications/2025/11/20/korean-government-should-push-against-the-misleading-fairness-act/>.
  76. Atkinson, Testimony Before House Ways and Means Committee.
  77. Mira Burri, María Vásquez Callo-Müller, and Kholofelo Kugler, “The Evolution of Digital Trade Law: Insights from TAPED,” *World Trade Review* 23, no. 2 (May 2024): 190-207, <https://www.cambridge.org/core/journals/world-trade-review/article/evolution-of-digital-trade-law-insights-from-taped/8C9B4DA7D7FA50B10913BD7575929750>.
  78. Atkinson et al., “Letter to the Trump Administration Regarding Non-Tariff Attacks.”
  79. Robert D. Atkinson, “Go to the Mattresses: It’s Time to Reset U.S.-EU Tech and Trade Relations” (ITIF, October 21, 2024), <https://itif.org/publications/2024/10/21/its-time-to-reset-us-eu-tech-and-trade-relations/>.
  80. Patrick Leblond, “After USTR’s Move, Global Governance of Digital Trade Is Fraught with Unknowns” (Centre for International Governance Innovation, December 9, 2023), <https://www.cigionline.org/articles/after-ustrs-move-global-governance-of-digital-trade-is-fraught-with-unknowns/>.
  81. John G. Murphy, “Digital Commerce at the Crossroads: The Case for a Digital Trade Agreement” (U.S. Chamber of Commerce, August 17, 2021), <https://www.uschamber.com/international/trade-agreements/digital-commerce-at-the-crossroads-the-case-for-a-digital-trade-agreement>.
  82. Rachel F. Fefer, Shayerah I. Akhtar, and Michael D. Sutherland, “Digital Trade and U.S. Trade Policy” (Congressional Research Service, December 9, 2021), <https://sgp.fas.org/crs/misc/R44565.pdf>.
  83. Hilal Aka, “Tip of the Iceberg: Understanding the Full Depth of Big Tech’s Contribution to US Innovation and Competitiveness” (ITIF, October 2025), <https://itif.org/publications/2025/10/06/tip-of-the-iceberg-understanding-big-techs-contribution-us-innovation-competitiveness/>.
  84. Pablo Chavez, “Sovereign AI in a Hybrid World: National Strategies and Policy Responses,” Lawfare, November 7, 2024, <https://www.lawfaremedia.org/article/sovereign-ai-in-a-hybrid-world--national-strategies-and-policy-responses>.
  85. Ronn Torossian, “How AI Infrastructure Will Redefine National Sovereignty,” Built In, June 9, 2025, <https://builtin.com/articles/ai-infrastructure-national-sovereignty>.
  86. Ibid.

87. “Sovereignty, Security, Scale: A UK Strategy for AI Infrastructure” (Tony Blair Institute, July 29, 2025), <https://institute.global/insights/tech-and-digitalisation/sovereignty-security-scale-a-uk-strategy-for-ai-infrastructure>.
88. U.S. International Development Finance Corporation, *Annual Report 2024* (Washington DC: U.S. International Development Finance Corporation, 2024), [https://www.dfc.gov/sites/default/files/media/documents/DFC\\_AnnualReport\\_2024\\_v6.pdf](https://www.dfc.gov/sites/default/files/media/documents/DFC_AnnualReport_2024_v6.pdf).
89. Robert D. Atkinson, “US Development Financing Needs to Stop Rewarding Nations Whose Policies Harm US Companies and Workers” (ITIF, August 12, 2024), <https://itif.org/publications/2024/08/12/us-development-financing-stop-rewarding-nations-policies-harm-us-companies/>.
90. U.S. International Development Finance Corporation, FY2022-2026 Strategic Plan; Erin Murphy and Daniel F. Runde, “The Next Five Years of the DFC: Ten Recommendations to Revamp the Agency” (Center for Strategic and International Studies, January 10, 2025), <https://www.csis.org/analysis/next-five-years-dfc-ten-recommendations-revamp-agency>.
91. Erin Murphy, “A New Chapter for the U.S. International Development Finance Corporation” (Center for Strategic and International Studies, January 2025), <https://www.csis.org/analysis/new-chapter-us-international-development-finance-corporation>; Nisha Biswal, Elaine Dezenski, and Ambassador John A. Simon, “Supercharging the Development Finance Corporation: Opportunities and Pathways for Development, Infrastructure, and Investment” (Foundation for Defense of Democracies event, July 11, 2024), <https://www.fdd.org/events/2024/07/11/supercharging-the-development-finance-corporation-opportunities-and-pathways-for-development-infrastructure-and-investment/>.
92. Atkinson, “Testimony Before House Ways and Means Committee.”
93. Ibid.
94. Hosuk Lee-Makiyama and Badri Narayanan Gopalakrishnan, “The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions” (European Centre for International Political Economy, 2019), <https://ecipe.org/publications/moratorium/>.
95. U.S. Department of State, “United States International Cyberspace and Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future,” May 6, 2024, <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>; U.S. Government Accountability Office, “Cyber Diplomacy: The Bureau of Cyberspace and Digital Policy’s Efforts to Advance U.S. Interests,” GAO-25-108445, April 29, 2025, <https://www.gao.gov/products/gao-25-108445>.
96. “Achieving Europe’s Cloud and Data Sovereignty,” Élysée, November 18, 2025, <https://www.elysee.fr/en/emmanuel-macron/2025/11/18/achieving-europes-cloud-and-data-sovereignty>.
97. “Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?” *Global Studies Quarterly*, January 27, 2024, <https://academic.oup.com/isagsq/article/4/1/ksad077/7590537>; “Cyber Sovereignty and the PRC’s Vision for Global Internet Governance,” Jamestown, November 19, 2020, <https://jamestown.org/program/cyber-sovereignty-and-the-prcs-vision-for-global-internet-governance/>; “Chinese notion of cyber sovereignty: Building an alternate digital order,” Observer Research Foundation, August 20, 2024, <https://www.orfonline.org/expert-speak/chinese-notion-of-cyber-sovereignty-building-an-alternate-digital-order>.
98. “Mapping the Brussels Effect: The GDPR Goes Global,” CEPA, September 13, 2025, <https://cepa.org/comprehensive-reports/mapping-the-brussels-effect-the-gdpr-goes-global/>.
99. “Cyber Sovereignty: How China is Changing the Rules of Internet Freedom,” UC Institute on Global Conflict and Cooperation, 2021, [https://ucigcc.org/wp-content/uploads/2022/06/2022\\_wp2\\_hulvey-FINAL.pdf](https://ucigcc.org/wp-content/uploads/2022/06/2022_wp2_hulvey-FINAL.pdf); “Global AI Governance Action Plan,” Permanent Mission of the People’s Republic of

China to the UN, July 29, 2025, [https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729\\_11679232.htm](https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729_11679232.htm).

100. Atkinson, “Testimony Before House Ways and Means Committee”; Atkinson et al., “Letter to the Trump Administration Regarding Non-Tariff Attacks.”
101. Atkinson, “Testimony Before House Ways and Means Committee.”
102. Atkinson, “Go to the Mattresses: It’s Time to Reset U.S.-EU Tech and Trade Relations;” Espinoza, “EU should focus on top 5 tech companies, says leading MEP.”
103. Aka, “EU Regulatory Actions Against US Tech Companies Are a De Facto Tariff System.”; Joseph V. Coniglio and Lilla Nóra Kiss, “Comments to the Italian Competition Authority Regarding Draft DMA Enforcement Regulation” (ITIF, July 2024), <https://itif.org/publications/2024/07/11/comments-italian-competition-authority-draft-dma-enforcement-regulation/>.
104. Atkinson, “Testimony Before House Ways and Means Committee.”
105. Atkinson, “Go to the Mattresses: It’s Time to Reset U.S.-EU Tech and Trade Relations.”
106. Nigel Cory, “How the United States and CPTPP Countries Can Stop Vietnam’s Slide Toward China-Like Digital Protection and Authoritarianism” (ITIF, September 2023), <https://itif.org/publications/2023/09/08/how-the-united-states-and-cptpp-countries-can-stop-vietnams-slide-toward-china-like-digital-protection-and-authoritarianism/>.
107. Atkinson, “Testimony Before House Ways and Means Committee.”
108. Ibid.
109. Mira Burri, “Data Flows and Global Trade Law,” in Mira Burri, ed., *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 11–41, <https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-flows-and-global-trade-law/E98D121FC172A9F534DE9C310919E389>; Patrick Leblond, “Trade Agreements and Data Governance” (Centre for International Governance Innovation, November 12, 2024), <https://www.cigionline.org/articles/trade-agreements-and-data-governance/>.
110. Atkinson, “Go to the Mattresses: It’s Time to Reset U.S.-EU Tech and Trade Relations.”
111. Ibid.
112. Singham and Abbott, *Trade, Competition and Domestic Regulatory Policy*; Singham, *International Trade, Regulation and the Global Economy: The Impact of Anti-Competitive Market Distortions*. The Anti-Competitive Market Distortions (ACMD) model provides a methodology for quantifying economic harm from regulatory measures that deviate from sound competition principles, enabling proportional calibration of remedies based on measured damage to U.S. markets. See Compete Foundation, <https://www.competerefoundation.org/>.
113. Atkinson, “Go to the Mattresses: It’s Time to Reset U.S.-EU Tech and Trade Relations”; “To Do: Impose Mirror Taxes on Countries With Digital Service Taxes” (ITIF, September 20, 2024), <https://itif.org/publications/2024/09/20/to-do-impose-mirror-taxes-on-countries-with-digital-service-taxes/>.