



March 31, 2025

Trump Administration 2025 “National Trade Estimates” Report Attacks as Illegal Trade Barriers Other Nations’ Data Security, Privacy, and Other Digital Policies Enacted Here by Congress and State Legislatures

Will Trump Administration Side with Big Tech and Against Sovereignty to Weaponize Trade to Internationally Preempt Domestic Laws?

On March 31, 2025, the Office of the U.S. Trade Representative (USTR) published the statutorily-required annual National Trade Estimates (NTE) report of what ostensibly are trade-partner countries’ illegal trade barriers. The NTE, which is based in part on policies brought to USTR’s attention through a formal request for private sector input, has been used by corporations and their lobbyists to translate other countries’ public interest policies that various industries dislike into an official communication about what the U.S. government deems to be illegal trade barriers.

During Democratic and Republican presidencies alike, the NTE listed other countries’ food safety, environmental, affordable medicine access, and other policies. **Listing a policy in the NTE armed industry interests to attack an array of similar policies domestically.** Digital policies were only added in 1998, when the Internet Tax Freedom Act added “barriers to United States electronic commerce” to be covered by the NTE. This opened the door for Big Tech interests to demand that U.S. government officials elevate their private peeves against digital governance policies adopted by other nations into official U.S. trade policy. In 2022, Rethink Trade published a study analyzing Big Tech submissions to the Federal Register NTE docket. “*Digital Trade” Doublespeak: Big Tech’s Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies,*” provided a guide in unguarded language to the digital oversight policies that the Big Tech lobby sought to kill.¹ The report exposed what the Big Tech lobby sought to soft pedal as their “digital trade” agenda to be an effort to weaponize trade to evade accountability.

The dangerous practice of listing every corporate complaint about another country’s domestic policies in the NTE largely stopped during the Biden administration, when USTR targeted policies that discriminate against U.S. products and firms or otherwise violated trade principles. The corporate lobby was furious and attacked USTR. In 2025, under the Trump administration, the NTE has again become a government-sponsored corporate hit list of any policy some U.S. company or lobbyists dislikes. This day-off initial NTE analysis compiles key policies relating to online privacy, data security, Big Tech anti-monopoly, and other digital matters listed in the 2025 report. Notably, almost none of these policies were listed during the Biden administration.

The overview:

- At least 10 attacks to GDPR-style data privacy regimes: Brazil, Chile, Ecuador, EU, Israel, South Korea, Norway, Peru, Switzerland, and Uruguay.
- At least, 5 attacks on digital competition policies, such as platform-outlet bargaining codes.

¹ Daniel Rangel, Taylor Buck, Erik Peinert and Lori Wallach, ““Digital Trade” Doublespeak: Big Tech’s Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies,” Rethink Trade, November 2022. <https://rethinktrade.org/wp-content/uploads/2022/11/20221101-AELP-DocLayout-v7.pdf>

- Criticism of the EU’s AI Act rules that provides for source-code examination.

Some key excerpts from the report:

- From the outset, when giving examples of potential “digital trade barriers” the 2025 NTE report includes: “barriers to cross-border data flows, discriminatory practices affecting trade in digital products, restrictions on the provision of Internet-enabled services, and other restrictive technology requirements.”
- On Australia, the 2025 NTE report brought back the criticism of Australia’s landmark Media Bargaining Code: “On March 2, 2021, the Australian Government passed the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021 (Bargaining Code). Under the Bargaining Code, designated platform services companies are required to engage in negotiations with registered Australian news media businesses to pay the news businesses for content accessed via certain services offered on the companies’ digital platforms. In December 2024, the Government announced its intent to tighten the rules surrounding the Bargaining Code, including by introducing a financial penalty for designated platforms that do not reach or renew commercial agreements. The United States continues to monitor this issue.”

Following are key digital policy excerpts from the country-by-country listing.

Brazil:

- “The Brazilian Government charges a flat 60 percent duty for all express shipments imported through the Simplified Customs Clearance process. The Simplified Customs Clearance process limits commercial shipments to \$100,000 per importer per year. Moreover, Brazilian Customs has established express delivery maximum per-shipment value limits of \$10,000 for exports and \$3,000 for imports.”
- **“Personal Data Protection Regulation:** Brazil’s General Law for the Protection of Personal Data (LGPD) includes provisions concerning restrictions on the transfer of personal data outside of Brazil. The regulations implementing these restrictions were published in August 2024, with a 12-month transition period for companies. Delayed implementation of approved mechanisms for international data transfers (e.g., certifications, codes of conduct, and contractual clauses) has created uncertainty for businesses and obstacles to the routine processing and sharing of data for business purposes. The United States has encouraged Brazil to work closely with companies and organizations affected by the LGPD to resolve implementation and enforcement issues in a reasonable and consistent manner.”

Canada:

- “On June 20, 2024, Canada enacted a digital services tax (DST), imposing a three percent levy on certain gross revenues relating to online marketplaces, online targeted advertising, social media platforms, and user data. The DST entered into force on June 28, 2024. Canada’s DST is retroactive to January 1, 2022, and companies are required to remit payments starting on June 30, 2025. The DST applies to taxpayers with annual global revenues of €750 million (approximately \$833 million) and Canadian digital services revenue of CA\$20 million (approximately \$14.3 million). As the United States noted in comments to Canada in 2021 and 2023, most DSTs have been designed in ways that discriminate against U.S. companies, as they single out U.S. firms for taxation while effectively excluding national firms engaged in similar lines of business.”

- “On June 22, 2023, the Canadian Government passed the Online News Act (Bill C-18). Under the Act, designated platform services companies are required to engage in negotiations with Canadian news providers to pay the news businesses for content accessed via certain services offered on the companies’ digital platforms. The Act gives the CRTC new powers to regulate the Canadian news industry, including determining who is a journalist, what is an eligible news business, and calculating compensation. The United States continues to monitor this issue.”

Chile:

- “INTELLECTUAL PROPERTY PROTECTION: Chile remained on the Priority Watch List in the 2024 Special 301 Report. The United States remains concerned about the adequacy and effectiveness of the protection and enforcement of IP rights in Chile and about the implementation of certain IP obligations under the FTA. Longstanding concerns remain about protections against the unlawful circumvention of technological protection measures, failure to ratify the 1991 Act of the International Convention for the Protection of New Varieties of Plants (UPOV 1991), and an ineffective internet service provider liability regime that has failed to promote effective and expeditious action against online piracy. The United States also continues to urge Chile to address certain aspects of its FTA commitments on satellite piracy. In addition, pharmaceutical stakeholders continue to raise concerns over the efficacy of Chile’s system for resolving patent issues expeditiously in connection with applications to market pharmaceutical products and over the provision of adequate protection against unfair commercial use, as well as unauthorized disclosure, of undisclosed test or other data generated to obtain marketing approval for pharmaceutical products. The United States also continues to encourage Chile to provide transparency and due process to all interested parties in connection with potential recognition or protection of geographical indications, including in connection with trade agreement negotiations.”
- “ELECTRONIC COMMERCE / DIGITAL TRADE BARRIERS Chile published its Data Protection Law (DPL) in December 2024. The law requires countries to which data will be transferred to demonstrate “adequate” levels of data protection comparable to privacy standards in Chile. In the absence of a determination on a country’s data protection standards, companies are required to use approved contractual clauses to transfer data. U.S. stakeholders have expressed concerns that the guidelines for using contractual clauses are unclear and the lack of clear definitions for key concepts is creating uncertainty for companies. The United States continues to engage with Chile, including through participating in multilateral data privacy certification arrangements, which provide a mechanism for companies to facilitate international transfers of personal data in compliance with the laws of participating jurisdictions.”

Colombia:

- “ELECTRONIC COMMERCE / DIGITAL TRADE BARRIERS Colombia brought its Significant Economic Presence (SEP) tax into force on January 1, 2024, per Article 57 of Law 2277 of 2022. The tax applies to the sale of tangible goods and digital services. A non-resident entity has SEP status and is subject to the tax if: 1) it has deliberate and systematic interaction with the Colombian market (defined, in part, as maintaining a marketing interaction with 300,000 or more customers in Colombia); and 2) it obtains gross income of at least “31,300 Tax Value Units” (for 2025, approximately \$370,000) from transactions involving the sale of goods or services in the Colombian market. Non-residents with an SEP in Colombia pay a 3 percent tax on gross income if they register and file in Colombia or a

withholding tax of 10 percent. Prior to the tax reform's passage in 2022, the United States raised with Colombia its concerns regarding the differing application of the rule to non-residents and residents."

Ecuador:

- **"Data Localization:** The Law for the Development of Technological Financial Services (Fintech Law) came into force in December 2022. The Fintech Law amended Article 146 of the Ingenuity Code, which had previously required the localization of strategic sector and national security data. The reform established a classification of data that includes open, reserved, and confidential data. While the Fintech Law maintains data localization requirements for reserved and confidential data, it eliminated the localization requirement for other categories of data. Consequently, companies will now be able to provide storage services for some Ecuadorian data from data centers outside Ecuador. However, under the Ministry of Telecommunications (MINTEL) Agreement 141 of 2011, customers must contract with cloud services providers that rely on data centers outside Ecuador through the National Telecommunications Corporation (CNT), a state-owned company, as a local partner."
- **"Personal Data Protection:** In May 2021, Ecuador's first Personal Data Protection Law went into effect. On March 28, 2024, Ecuador appointed a Personal Data Protection Superintendent to implement the law. The law establishes that Ecuadorian personal data can only be transferred to organizations or territories that provide adequate levels of protection, a standard yet to be defined by the regulating body creating regulatory uncertainty for U.S. companies. The law also establishes fines on data protection infractions that will come into force in the near term. The penalties range between 0.7 percent and one percent of revenues, based on business volume. The Superintendency issued resolution No. SPDP-2024-0002-R on September 6, 2024 to establish a technical guide for the registration of special proxies for foreign data controllers and data processors that perform personal data processing activities. Resident and non-resident companies had six months (i.e., until March 2025) to comply with these requirements. The United States is committed to working with Ecuador on data protection and privacy issues including conversations to ensure mutual participation in multilateral data privacy certification arrangements that provide a mechanism for companies to facilitate international transfers of personal data in baseline compliance with the laws of participating jurisdictions."

Egypt:

- **"ELECTRONIC COMMERCE / DIGITAL TRADE BARRIERS:** Egypt's Personal Data Protection Act, Law No. 151/2020, requires licenses for cross-border data transfers. The United States is monitoring the implementation of this law and its draft regulations, which are expected to be implemented by the Data Protection Authority. The Data Protection Authority had not been established as of October 2024. The United States has engaged with Egypt regarding best practices for privacy and data security through technical assistance engagements in September 2023 and June 2024, and will continue to engage with Egypt through various bilateral and multilateral fora."

El Salvador:

- **"Data Localization Requirements:** On August 17, 2021, the Legislative Assembly passed amendments to the Credit History Law. The amendments introduced data localization

requirements mandating credit bureaus and economic agents that report on credit history to store data exclusively in El Salvador and grant unrestricted access to the Central Bank and the Superintendence of the Financial System. U.S. stakeholders have expressed concerns that these requirements could compromise consumer data privacy and protection. The United States continues to engage El Salvador on this issue.”

European Union:

- **“Eco-design for Sustainable Products Regulation and the Digital Product Passport:** On July 18, 2024, the Eco-design for Sustainable Products Regulation (Regulation (EU) 2024/1781) entered into force. The regulation establishes an eco-design framework for sustainable products that will require industry to meet new sustainability requirements. Articles 7 through 15 of the regulation require industry to develop and implement a new digital label (known as a Digital Product Passport or DPP) to trace lifecycle information and other aspects of a product in order to inform consumers and help public authorities to better perform checks and controls. Some U.S. stakeholders are concerned that the DPP requirements set unrealistic implementation timelines and do not include sufficient safeguards to prevent the unauthorized disclosure of confidential business information. The United States made multiple requests to the EU to notify the measure to the WTO to allow trading partners the opportunity to provide feedback. To date, the EU has refused to notify the measure.”
- **“Proposed EU Cybersecurity Certification Scheme for Cloud Services:** The EU is considering a new cybersecurity certification scheme for cloud services, (EUCS). The draft scheme is under discussion between cybersecurity security experts of the EU Member States, the European Commission, and the European Union Agency for Cybersecurity. Once finalized, the EUCS is expected to be mandatory for parts of the public sector and possibly select private sector cloud services. The latest EUCS draft that is publicly available eliminates the sovereignty criteria and the requirement of data storage in the EU as necessary criteria to be certified at the highest level of cybersecurity. However, these changes face opposition from the French data protection authority, the Commission Nationale de l’Informatique et des Libertés (CNIL), and the French parliamentary Committee for Digital Postal Affairs. France is expected to advocate for stricter requirements in future debates within the EU. The EU covers cloud services in their GPA schedule and is required to offer non-discriminatory access to U.S. and other GPA suppliers for covered procurements. The United States has presented its concerns about these policies in the WTO Committee on Government Procurement and in bilateral meetings with EU officials.”
- **“Member State Measures on Cloud Services • France:** France’s national digital security agency, Agence Nationale de la Securite des Systemes d’Information (ANSSI), maintains a security certification scheme for cloud services, commonly referred to as SecNumCloud. In May 2021, the French Government issued a strategy for the use of cloud computing by the state (Trusted Cloud strategy), requiring that government agencies and commercial entities considered “critical” must select only cloud services vendors with a SecNumCloud certification to handle their highly sensitive data. As part of this strategy, ANSSI published in March 2022 a revision to the SecNumCloud certification requirements. This revision requires that any cloud provider that handles “highly sensitive” data must be at least 61 percent EU-owned and “immune” from non-EU laws. France’s Prime Minister signed an official circular on May 31, 2023, defining “sensitive data” to which SecNumCloud certification

requirements apply. The vague definition of “sensitive data” could lead foreign cloud services suppliers to be increasingly precluded from providing cloud services to French public authorities. • Hungary: State and local government bodies and organizations are only allowed to process data in systems operated in the territory of Hungary. Electronic information systems can only be hosted in EU Member States for organizations providing services deemed as critical, which include energy, transportation, agriculture, and health industries.”

- “The **Digital Services Act (DSA)** entered into force on November 16, 2022. The DSA is intended to regulate certain online services, including through rules for how content is shared online. U.S. stakeholders have expressed concerns that the DSA’s adoption of a framework for limitations of liability included modifications to the eligibility threshold and conditions that had been set in the E-Commerce Directive, which may adversely impact their intellectual property (IP) rights, in particular for copyright and trademarks.
- “The **Data Act** entered into force on January 11, 2024 and seeks to maximize the value of data and promoting innovation by increasing the transfer of data that is stored within devices and applications. The Data Act requires the disclosure and making available of data that may be protected by the data holder’s or a third party’s trade secrets, copyright, or other IP.
- “The **Artificial Intelligence (AI) Act** entered into force on August 1, 2024 with various obligations applying at later stages. It aims to provide a risk-based approach to regulating the development, deployment, and use of AI-driven products, services, and systems. Stakeholders have concerns regarding the implementation of the Act related to source code, trade secrets, and copyright protection, including the requirement to comply with EU copyright law. The United States will continue to monitor developments.”
- “**Digital Services Act:** The Digital Services Act (DSA) entered into force in November 2022, and took effect on February 17, 2024, with certain provisions already in effect on November 16, 2022. The DSA provides the Commission authority to regulate the business practices of certain large digital services suppliers, designated as “Very Large Online Platforms” (VLOPs), which include online platforms with “average monthly active recipients of the service” in the EU equal to or higher than 45 million (this number will be adjusted by the EU in the future to ensure it corresponds to 10 percent of the EU population). The DSA also imposes strict transparency and reporting obligations and audit requirements, and requires VLOPs to address “systemic risks” present in their services. The DSA defines systemic risks as the dissemination of illegal content, any negative effects for the exercise of certain fundamental rights, and intentional manipulation of the service. A VLOP has to consider how its content moderation systems, recommendation systems, and systems for displaying advertisements, influence these risks and enact mitigation measures for any systemic risks. Once a platform is designated as a VLOP by the Commission, the platform has four months to come into compliance with its obligations under the DSA. The DSA provides the Member States and the Commission with the authority to impose fines not exceeding six percent of the total annual turnover of a VLOP and in some instances can impose a periodic fine of up to 5 percent of average daily global turnover for each day a VLOP fails to comply with a remedy, interim measure, or commitment imposed by the Commission. In certain instances, the Commission can also order a VLOP to suspend its operations in the EU. The DSA also provides the Commission with the power to adopt

“delegated acts” for portions of the DSA, granting the Commission expansive authority to adopt additional regulation. On April 25, 2023, the European Commission designated the first set of VLOPs. **The majority of designated VLOPs are U.S. firms, resulting in regulatory burdens that disproportionately affect U.S. firms.**”

- **“Digital Markets Act:** The Digital Markets Act (DMA) entered into force in November 2022 and took effect in May 2023. The DMA provides the Commission with authority to regulate the business practices of certain large digital services suppliers, designated as “gatekeepers. (...) The “gatekeepers” designated by the DMA disproportionately capture U.S. firms compared to their EU competitors, and therefore undermine U.S. competitiveness in the European market by increasing the compliance costs on certain U.S. firms while not placing a similar burden on EU competitors. The Commission is currently investigating U.S. firms and has imposed excessive fines for violating the DMA.”
- **“Data Act:** The Data Act entered into force in January 2024, and its rules will go into effect on September 12, 2025. The Act establishes rules for access and use of both personal and non-personal data by businesses, consumers, researchers, and public sector bodies, including data generated by connected devices and digital services. The Act applies to the transfer or “sharing” of business-to-business, business-to-consumer, and business to-government non-personal data that is stored within industrial applications (e.g., robots, wind farms) and smart devices (e.g., smart TVs, connected cars). The Data Act regulates the rights of users (in many cases meaning the generators of such data, like the users of smart TVs or drivers of connected cars) to access data that these connected machines or devices generate. The Data Act also mandates certain sharing of this data with third parties, including researchers, public sector bodies, and other private companies. Firms may only refuse access to data covered by trade secrets in exceptional circumstances, but can require the users and third parties to preserve the confidentiality of data considered to be trade secrets. Additionally, the Data Act requires cloud service and other data processing service providers to remove obstacles for customers terminating their service. On international transfers of non-personal data, the rules oblige providers of such services to take “all reasonable technical, legal and organizational measures, including contractual arrangements” to prevent international transfers or governmental access to non-personal data that are in conflict with EU or Member state law. This may impose burdensome requirements on U.S. service providers and undermine the ability of U.S. providers of such services to compete in the European market.”
- **“Data Localization:** The GDPR took effect in May 2018. The GDPR restricts the transfer of the personal data of EU “data subjects” (any natural person whose personal data is being processed) outside of the EU, except to specific countries that the EU has determined provide adequate data protection under EU law or when other specific requirements are met, such as the use of standard contractual clauses (SCCs) or binding corporate rules. Restrictions on the flow of data have a significant effect on the conditions for the cross-border supply of numerous services and for enabling the functionality embedded in intelligent goods (i.e., smart devices), among other effects. Due to the EU’s assertion of extraterritorial jurisdiction for the GDPR, as well as the GDPR’s broad impact on many areas of the economy, U.S. companies have expressed concerns that there remains a need for clear and consistent guidance in the implementation and enforcement of the GDPR.”

Israel:

- **“Data Localization Requirements:** Data protection in Israel is governed primarily by the Protection of Privacy Law (5741-1981) and the guidelines of the Israeli regulator, the Privacy Protection Authority. Similar to the EU General Data Protection Regulation, Israeli law restricts the cross-border transfer of personal data of Israelis unless certain specific criteria are met, such as the use of standard contract clauses. Since July 2023, Israel recognizes the EU–U.S. Data Privacy Framework as a valid mechanism to meet Israeli requirements for the protection of personal data. (For further information on the EU’s General Data Protection Regulation and the EU–U.S. Data Privacy Framework, see the Electronic Commerce / Digital Trade Barriers section of the EU Chapter of this NTE Report.)”

Japan:

- **“Digital Platform Regulation:** In 2019, the Digital Market Competition Headquarters (DMCH), was created under the Cabinet Secretariat to lead the coordination of competition policy in the digital market. U.S. companies have expressed concern that they are being subjected to additional regulations and scrutiny that do not apply to most Japanese conglomerates, some of which operate in similar sectors. In December 2019, the JFTC released guidelines on applying the Antimonopoly Act (AMA) to transactions between digital platform operators and consumers. In these guidelines, the JFTC asserts that platform companies are in “a superior bargaining position” when customers have no choice but to provide their data to use the services and platform companies may commit an abuse of that position when use of personal data is not fully and accurately disclosed or personal data is not protected. After receiving input from stakeholders concerned about insufficient guidance, the JFTC provided several examples of practices that would or would not constitute an abuse of superior bargaining position. The Act on Improving Transparency and Fairness of Digital Platforms (the Digital Platform Act) imposes additional obligations on large companies designated by METI as “specified digital platform providers” for specific services, including “general online shopping malls selling goods,” “application stores,” “mediaintegrated digital ad platforms,” and “ad intermediary digital platforms.” The “specified digital platform providers” designated by METI have disproportionately captured U.S. firms compared to their Japanese and third country competitors and therefore undermine U.S. competitiveness in Japan by increasing the compliance costs on certain U.S. firms while not placing a similar burden on their competitors.”

Kenya:

- “On December 27, 2024, Kenya replaced its digital services tax with a “significant economic presence tax” under the Tax Laws (Amendment) Act of 2024. A three percent effective tax rate on gross revenues is imposed on non-residents whose revenue from the provision of services is derived from or accrues in Kenya through a digital marketplace. Those excepted from the application of the tax include non-residents who offer services through a permanent establishment in Kenya or have an annual turnover of less than 5 million Kenyan Shillings (approximately \$38,800).”
- “Data Localization Requirements Kenya’s 2019 Data Protection Act (DPA) includes unclear provisions governing the cross-border transfer of personal information. The DPA requires that either data subjects provide consent for transfers outside Kenya or controllers provide proof that personal data will be secure as a condition for transferring the data outside Kenya,

but does not describe what would constitute acceptable proof. The 2021 Data Protection regulations require companies processing personal data “for the purpose of actualizing a public good” to be processed in a data center located and maintain in Kenya at least one copy of the personal data used.”

Korea:

- “In 2024, the Korean Government, including the Korea Free Trade Commission and the National Assembly, considered proposals to regulate certain suppliers of digital services that meet global and national revenue thresholds. These proposals would apply to a number of large U.S. companies operating in the Korean market. The proposals also appear to apply to two large Korean companies, but exclude a number of other major Korean companies as well as companies from other countries. The proposals include a number of ex ante prohibitions and obligations that would apply to companies to address competition issues in the Korean market. U.S. companies have urged the Korean Government to take a more deliberative approach to these issues, including by conducting a comprehensive market analysis to assess the level of competition and a regulatory impact assessment of the proposed measures. The United States continues to urge Korea to improve its engagement with this sector by enhancing transparency and providing meaningful opportunities for stakeholder input.”
- **“Location-Based Data:** Korea’s restrictions on the export of location-based data have led to a competitive disadvantage for international suppliers seeking to incorporate such data into services offered from outside Korea. For example, foreign-based suppliers of interactive services incorporating location-based functions, such as traffic updates and navigation directions, cannot fully compete against Korean companies because locallybased competitors typically are not dependent on foreign data processing centers and do not need to export location-based data. Korea is the only significant market in the world that maintains such restrictions on the export of location-based data. While there is no general legal prohibition on exporting location-based data, exporting such data requires a license. As of December 31, 2024, Korea had never approved a license to export cartographic or other location-based data, despite receiving numerous applications from foreign suppliers.”
- **“Data Localization:** The 2011 Personal Information Protection Act (PIPA) imposes restrictions on the transfer of personal data outside Korea. In 2023, the PIPA was substantially revised, and the Korean Personal Information Protection Commission (PIPC) adopted an Enforcement Decree that took effect in March 2024. These changes provide the PIPC with new authority to impose fines on service providers based on their global revenue rather than revenue in Korea, and to order the suspension of cross-border transfer of personal data. The PIPA permits the transfer of personal data outside of Korea only in limited circumstances, such as when the service provider has obtained a separate consent from the data subject to transfer data outside of Korea, when the recipient of the data has obtained a privacy certification recognized by the PIPC, or when the data is transferred to a country that the PIPC has determined provides an equal level of data protection, among others. These restrictions pose barriers to the cross-border provision of based services that depend on data storage and processing.”

Nigeria:

- **“Data Localization:** The National Information Technology Development Agency (NITDA) Guidelines for Nigerian Content Development in Information and Communication

Technology require all foreign and domestic businesses to store all data concerning Nigerian citizens within Nigeria. The NITDA Guidelines further require that businesses host all government data locally, unless officially exempted. However, the requirements do not seem to be rigorously enforced which causes uncertainty for businesses seeking to comply with the requirements.”

Norway:

- **“Data Localization Requirements:** Data protection in Norway is governed by the Norwegian Personal Data Act, which implements the European Union General Data Protection Regulation (GDPR) and became effective on July 10, 2018. The GDPR was incorporated into the EEA Agreement on July 6, 2018. The Norwegian Personal Data Act restricts the transfer of the personal data outside of the EEA, except to specific countries determined to provide adequate data protection by the European Commission (Commission) or when other specific requirements are met, such as the use of standard contract clauses or binding corporate rules. Restrictions on the flow of data have a significant effect on the conditions for enabling the functionality embedded in intelligent goods (i.e., smart devices).”

Panama:

- **“Data Localization:** Panama’s Government Innovation Authority resolutions 52 and 03 required all cloud services used by government entities for mission critical work and “sensitive” data hosted on servers outside the country to relocate to Panama by December 31, 2024. The scope of mission critical work and sensitive data subject to the resolutions remains unclear. The United States will continue to monitor the status of these resolutions and seek clarifications from Panama, where necessary.”

Peru:

- **“Personal Data Protection:** The Personal Data Protection Law 29733(PDPL) and the Supreme Decree 003-2013-JUS-Regulation of the PDPL (Regulation) are the primary data protection laws in Peru. Peru’s data protection laws allow crossborder data transfers to countries determined to have the same or adequate level of data protection as Peru. In the absence of this determination, organizations are required to use standard contractual clauses and other measures to transfer data outside of Peru. Despite repeated requests, Peru has yet to initiate the formal adequacy assessment process with the United States. Without an adequacy determination, U.S. companies face increased costs, fragmented operations, and may be forced to localize data in Peru. The United States remains committed to working with Peru on data protection and privacy issues including conversations to ensure mutual participation in multilateral data privacy certification arrangements that provide a mechanism for companies to facilitate international transfers of personal data for baseline compliance with the laws of participating jurisdictions.”
- “In 2020, the Digital Government Secretariat of Peru released Emergency Decree 007 – Digital Trust Framework draft regulations for consultation. The decree gives preferential treatment to domestic data storage and domestic service providers and includes: (1) the creation of a whitelist of permitted countries for cross-border transfer of data; (2) the issuance of digital security quality badges for private companies that serve as a governmental cybersecurity certification (ignoring the existence of global security standards); and (3) the creation of a national data center intended to host the information provided by the public sector entities and incentivize domestic storage of public data. The Digital Trust Framework

also includes broad definitions of digital services providers, failing to consider key differences among digital services and the differences in these services' ability to access client's information, or organizations that use digital channels to provide their services.”

Switzerland:

- “**Data Localization Requirements:** Swiss law restricts the transfer of personal data outside of Switzerland, except to which specific countries Switzerland has determined provide adequate data protection under Swiss law or when other specific requirements are met, such as the use of standard contract clauses or binding corporate rules. Restrictions on the flow of data have a significant effect on the conditions for enabling the functionality embedded in smart devices.”

Uruguay:

- “Law No. 18.331 on the Protection of Personal Data, the “Habeas Data” action, and Decree No. 414/009 govern personal data protection in Uruguay. Law No. 20075 entered into force on January 1, 2023, and amends the Uruguayan data protection system. Uruguayan law generally restricts cross-border transfers of personal data to countries and international entities unless certain specified conditions are met. The regulation implementing the law allows for the use of standard contract clauses, but U.S. companies report that uncertainty remains regarding whether companies can utilize certain tools or mechanisms to conduct cross-border data transfers.”

ANNEX: USTR Release

From: USTR Press <media@ustr.eop.gov>

Date: March 31, 2025 at 12:44:58 PM PDT

Subject: USTR Releases 2025 National Trade Estimate Report

Reply-To: USTR Press <media@ustr.eop.gov>

FOR IMMEDIATE RELEASE

March 31, 2025

USTR Releases 2025 National Trade Estimate Report

WASHINGTON – Today, the Office of the United States Trade Representative (USTR) submitted the 2025 National Trade Estimate (NTE) to President Trump and Congress. The NTE is an annual report detailing foreign trade barriers faced by U.S. exporters and USTR's efforts to reduce those barriers.

“No American President in modern history has recognized the wide-ranging and harmful foreign trade barriers American exporters face more than President Trump,” said Ambassador Greer. “Under his leadership, this administration is working diligently to address these unfair and non-reciprocal practices, helping restore fairness and put hardworking American businesses and workers first in the global market.”

The findings of the 2025 NTE underscore President Trump's America First Trade Policy and the President's 2025 Trade Policy Agenda.

To read the 2025 NTE, click [here](#).

The NTE is an annual report due to the President and Congress by March 31 of each year. USTR works closely with other government agencies and U.S. embassies and solicits comments from the public through a Federal Register Notice to prepare the NTE.

The annual report is submitted in accordance with Section 181 of the Trade Act of 1974, as added by Section 303 of the Trade and Tariff Act of 1984 and amended by Section 1304 of the Omnibus Trade and Competitiveness Act of 1988, Section 311 of the Uruguay Round Trade Agreements Act, and Section 1202 of the Internet Tax Freedom Act.

###