

Suggested Steps Thailand Could Take to Address Digital-Related Restrictions

Thailand Barriers to U.S. Digital Service Suppliers

Over the past several years, Thailand has passed or proposed several key measures that severely threaten the ability of U.S. digital service suppliers to access the Thai market: **burdensome reporting requirements for launch of new services; intrusive government intervention for content posted online**, through takedown orders and power to search and seize data and equipment; **proposed obligations for hosting content and marketplaces aligned with the EU’s *Digital Markets Act* and *Digital Services Act***; and **privacy rules that have extraterritorial reach** (all referenced below).

The net effect of these measures is undermining the presence of U.S. digital firms in the Thai market. Even where not directly or immediately restricting access, the burdens and risks associated with these measures will severely diminish market access opportunities now worth well over a [billion dollars](#) in this critical market that has significant growth potential—although only 39% of the population [used the internet](#) in 2015, that number has grown to 90% in 2023.

As the U.S. engages with Thailand to seek removal of trade impediments, several targeted changes could materially improve market access for U.S. suppliers, without requiring wholesale rewriting of legislation, by eliminating provisions that a) impose mandatory reporting procedures on U.S. products and services; b) subject U.S. services providers to onerous takedown regimes with threat of search and seizure of property; and c) propose to introduce *ex ante* restrictions on U.S. companies’ operations in-market.

Tangible Commitments from Thailand to Ease Digital Trade Barriers

Addressing existing barriers:

- Ensure greater flexibility for U.S. digital services providers under **Royal Decree on Digital Platform Services (B.E. 2565)**,¹ including removing obligations to notify the government prior to launch of certain business operations (Section 8 of the law) and additional requirements for larger services such as mandatory risk management systems and internal compliance managers (Section 19 of the law).
- Commit to **refrain from excessively ordering U.S. digital services providers to take down content** under the Computer Crime Act,² which empowers the Anti-Fake News Center³ to identify and require the removal of content it deems to be “false and misleading” (under Section 14(1) of the law) to protect broadly-defined “national security” concerns. **Similarly, commit to refrain from capriciously accessing U.S. companies’ systems.** The government is given power to “search and seize data and equipment in cases that are deemed issues of national emergency” under the 2018

¹ <https://www.eta.or.th/getattachment/Regulator/DigitalPlatform/law/Clean-Royal-Decree-on-DP-Corrected-1.pdf.aspx?lang=th-TH>.

² https://library.senate.go.th/document/mSubject/Ext64/64240_0001.PDF.

³ <https://www.antifakenewscenter.com/>.



amendments to the Cybersecurity Law.⁴

- **Issue formal guidance clarifying that data laws do not have extraterritorial reach over U.S. services providers.** Under the Personal Data Protection Act,⁵ all entities that collect, use, or otherwise share personal data in Thailand or of residents of the country are subject to the law. This creates liability for U.S. online services, as they may be subject to its reach if they decline to establish a business presence in Thailand but have Thai individuals who use their services.

Addressing proposed barriers:

- Commit to avoid enacting asymmetric online platform legislation, including the proposed **Platform Economy Act**,⁶ based on either *ex-ante* requirements or a presumption of illegal conduct that is applicable to only a subset of market participants, based on thresholds or service definitions that disproportionately affect U.S. firms—targeting U.S. online marketplaces, app stores, and other digital services. Any new proposals should focus on what is not regulated by existing laws and address regulatory gaps with specific, targeted legislation applicable to the entire industry, rather than broad, discriminatory measures.

Additional References

See CCIA comments on Thailand in its [submission for USTR’s 2025 National Trade Estimate](#) report. Among the laws discussed above, the Computer Crime Act was cited as a barrier to U.S. exports in USTR’s 2025 edition of the [report](#).

⁴ <https://www.globalcompliance.com/2018/12/23/thai-cybersecurity-bill-revised-november-2018-20181220/>; <https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/?guccounter=1>.

⁵ <https://www.dlapiperdataprotection.com/index.html?t=law&c=TH>.

⁶ <https://www.tilleke.com/insights/thailand-releases-draft-platform-economy-act-for-public-comment/>.