

Memorandum

From: Melinda St Louis, Director, Global Trade Watch, Public Citizen

Date: October 2026

Re: Coupang Corporation's Inappropriate Pressure Campaign to Weaponize U.S. Trade Policy Against South Korea's Digital Regulations

What is Coupang?

Coupang is a technology company that provides a range of online services — from retail (e-commerce) and food delivery to streaming and fintech. It was founded in 2010 by a U.S. citizen of Korean origin, Bom Kim, and is incorporated in Delaware, listed on the New York Stock Exchange, and headquartered in Seattle.

The company has been relatively unknown in the United States, as company filings indicate that it was [intended](#) to primarily serve the Korean market. To date, its primary business is in South Korea, with the company noting in recent [statutory filings](#) that “...over 90% of our total net revenues are from Korea.” The company's net revenues in 2025 were [\\$34.5 billion](#).

Coupang is owned by a consortium of investors, with the founder Bom Kim retaining significant voting power (though only ~9% of the company's equity). Notable shareholders include SoftBank (~17%, Japan), Baillie Gifford (~5%, UK), Greenoaks Capital (~3%, U.S.), Dodge and Cox (~4%, U.S.), BlackRock (~3.5%, U.S.) and Morgan Stanley (~2.5%, U.S.).

Why is Coupang in the news?

Coupang has faced a barrage of criticism and regulatory action in South Korea over a [massive data breach](#) in 2025 that reportedly compromised over 35 million user accounts. This was the biggest data breach in South Korean history.

Pursuant to an investigation that found inadequate data management systems and negligence, Coupang was [fined](#) over KRW 640 billion (approx. \$478 million) by South Korea's data protection authority — the Personal Information Protection Commission (PIPC) — earlier this year. This followed a separate [investigation](#)

conducted by the South Korean Government into the incident, which found mismanagement by the company.

Coupang has previously faced regulatory scrutiny by both the PIPC and South Korea's competition authority — the Korean Fair Trade Commission (KFTC). Coupang has also [been investigated](#) over its unethical [labor practices](#), some of which are alleged to have led to the [deaths of gig workers](#).

Washington Capitals Name Coupang as Jersey Partner Expanding American Business Worldwide

The NHL team's 2025-26 home jersey will feature Coupang's logo as both partners underscore digital exports and support...

How did Coupang's regulatory concerns in Korea become relevant to U.S. policymakers?

Coupang has enlisted all [available avenues](#) to [lobby](#) for U.S. lawmakers to pressure the South Korean government on its behalf (an expert quoted by [Politico](#) describes it as a “full court press”). The company:

- Spent \$2.27 million on [lobbying](#) in the U.S. since 2025, employing both in-house and outside lobbyists. It has [hired](#) former Trump administration officials such as Rob Porter and Kevin Warsh as its in-house lobbyists and employed Trump-associated lobbying firms for outside lobbyists, such as Ballard Partners and Miller Strategies.
- Employed 32 lobbyists, 3 in-house, with a 56% revolving door rate (former Trump officials or campaign associates).
- Joined three [lobbying trade associations](#): Computer and Communications Trade, National Foreign Trade Council, and US-Korean Business Council.
- Made \$200,000 in [campaign contributions](#) in 2025, mostly to relevant committee chairs.



- Donated \$1 million to [Trump's Inaugural Committee](#).
- Made a \$100,000 donation to another of Trump's vanity projects, the [Kennedy Center](#), in 2024.

Coupang's data breach starts drawing US legal attention

The Korea Times

This lobbying appears to have paid off.

- The House Judiciary Committee held a [hearing](#) in December 2025 purportedly focusing on how jurisdictions such as the EU and Korea are targeting U.S. tech companies by enforcing pro-competition regulations.
- More than 50 members of Congress addressed a [letter](#) to the South Korean government, advocating Coupang's cause in April 2026. Subsequently, several other members of Congress have raised [questions](#) or [written letters](#) to various U.S. authorities in this regard.
- Coupang's allegations that regulatory actions taken against it are discriminatory and motivated were echoed in a [report](#) released in July 2026 by the House Judiciary Committee. The report itself has been [dismissed](#) by the South Korean government, noting that it merely regurgitated Coupang's misleading claims.
- Marco Rubio [informed](#) the House Foreign Affairs Committee in June this year, in an apparent reference to the Coupang case, that South Korea's treatment of American companies has "affected our ability to finalize trade agreements."
- [Various trade experts](#) have pointed to how President Trump's decision to impose punitive tariffs on Korea was in part related to pressuring South Korea regarding the Coupang case. [Congresspersons](#) have also [made it clear](#) that tariffs are linked to South Korea's treatment of companies such as Coupang.

In January 2026, two of Coupang's U.S. investors, Greenoaks Capital and Altimeter Capital, issued a [notice of intent](#) to bring an Investor-State Dispute Settlement (ISDS) claim against South Korea under the U.S-Korea Free Trade Agreement (KORUS), alleging discriminatory and disproportionate attacks on the company. These attacks are alleged to have "erased billions of dollars of U.S. investment in Coupang." The proceeding was [subsequently joined](#) by three more U.S. investors, Foxhaven Capital,



Durable Capital and Abrams Capital. The KORUS requires a 90 day cooling off period before arbitration proceedings are commenced, and to date such proceedings [do not appear](#) to have been initiated. ISDS is a [controversial process](#), with [cross-party consensus](#) in the U.S. on the need to eliminate such provisions from trade and investment agreements.

[At the same time](#), Greenoaks Capital and Altimeter Capital filed a [petition under Section 301](#) of the Trade Act before the U.S. Trade Representative (USTR). This sought a finding from the USTR that South Korea's enforcement actions were discriminatory and arbitrarily restricted U.S. commerce. Such a finding would enable the imposition of punitive tariffs against South Korea.

How a simple consumer data breach spiralled into a national security crisis in US-South Korea relations

The Guardian

The petition was subsequently withdrawn, [reportedly](#) as the USTR is planning a broader investigation into South Korea's digital regulations. This, like the USTR's other recent S 301 investigations — into [Brazil's digital](#) and [other policies](#), supposed [failures to adequately ban forced labor](#) by 60+ countries, and Germany's [drug pricing policies](#) — is likely to be a sham proceeding, designed largely to enable the Trump administration to reimpose tariffs imposed under the International Emergency Economic Powers Act that were found illegal by the Supreme Court. The administration can then continue to pressure South Korea into acceding to U.S. deregulatory and other demands.

Are South Korean enforcement actions against Coupang discriminatory?

Over the past five years, Coupang has faced regulatory action in South Korea over several of its business practices, including (but not limited to):

- A KRW 3.297 billion fine by the Korean Fair Trade Commission (KFTC) in 2021 for [unfair treatment of suppliers](#);



- A KRW 162.824 billion fine by the KFTC in 2024 for [anti-competitive practices](#) such as self-preferencing and search manipulation;
- A KRW 1.59 billion fine by the PIPC in 2024 for [negligence with customer data](#) leading to a data breach.

These actions, together with the investigation into the 2025 data breach, are part of a broader swathe of regulatory action being undertaken by South Korean authorities to enforce competition and privacy laws in the South Korean digital ecosystem. However, these actions do not solely target Coupang and do not demonstrate any discriminatory intent on the part of the Korean authorities against U.S. companies.

As with many other jurisdictions, South Korea has worked to modernize its digital sector regulations over the last decade. This includes reform of its data protection law in 2020, when the PIPC was re-established as an independent regulator. This followed a modernization of the KFTC in 2019, when an independent enforcement unit was created to oversee digital competition concerns (the UK, amongst other countries, uses a similar system).

Both of these regulatory agencies have upped their enforcement actions over the past five years, against domestic and foreign companies alike. The PIPC has enforced South Korea's data protection law against companies such as Meta and Google, as well as large domestic companies such as SK Telecom. Similarly, the KFTC has taken action against several U.S. based companies such as Google, Oracle, Apple, and Meta, as well as South Korean tech companies such as Naver, Kakao, Nexon, NCSoft, and Smilegate.

Reportedly, Big Tech companies, [backed](#) by their [lobbyists](#), have [strategically exploited](#) the trade-law concept of "[non-discrimination](#)" to allege that virtually any [regulatory action](#) that targets U.S. companies is arbitrary or discriminatory despite evidence to the contrary. New age digital sector competition laws, such as the European Union's Digital Markets Act, have been regularly targeted by Big Tech companies. Similarly, they have attacked data protection and privacy laws [across the world](#), on grounds that they impose onerous and discriminatory obligations.

South Korean competition and data protection laws do not in fact discriminate against companies based on their country of origin. As has been pointed out [repeatedly](#), U.S. based tech companies have faced regulatory scrutiny because of their dominant position in the global Internet economy. Similarly, they tend to face comparatively larger fines as they have larger user bases, and therefore violations of the law can cause greater harm. As noted above, the most recent Coupang data breach was the largest in South Korean history. It affected almost 37 million user



accounts out of a population of ~50 million people. This inevitably led to significant public outcry, leading to government involvement and investigation of the matter, and the penalty imposed by the PIPC in its own proceedings.

Enforcement proceedings by the KFTC and PIPC, which are both independent regulatory bodies, provide Coupang the opportunity to present evidence and defend itself. Further, not every proceeding against Coupang has resulted in a fine. In some cases, regulators have imposed corrective measures requiring the company to amend particular business practices, while the KFTC has also resolved proceedings through its consent-decision procedure. This suggests that ensuring appropriate corporate conduct through adherence to public interest regulations is a central factor behind the Korean regulators' actions (as opposed to political motivations).

How does this fit into broader targeting of Korea's digital policies on behalf of U.S. Big Tech?

As mentioned, the attacks on South Korea's enforcement proceedings against Coupang follow a trend of U.S. based technology companies working with the U.S. government to coerce countries to implement favorable regulatory policies.

Public Citizen has documented the wide-ranging demands made by tech companies and their advocates to the USTR's [reciprocal tariffs report](#), as well as National Trade Estimate (NTE) Reports of [2025](#) and [2026](#). South Korean digital regulations have been frequently attacked by Big Tech companies, including its regulation of exports of geospatial, personal, and financial data, digital competition regulations, cybersecurity certification requirements for computer equipment and cloud services used by the public sector, and proposals for a network usage fee, amongst others.

Communications between industry groups and the USTR revealed through Public Citizen's [FOIA requests](#) and subsequent litigation indicate that Big Tech corporations and their trade associations are in constant dialogue with U.S. trade officials and are effectively driving the Trump administration's trade policy.

The disclosed communications indicate numerous and frequent meetings between tech industry groups and officials of the USTR, often timed to coincide with engagement between the U.S. and foreign governments, including that of South Korea. Big Tech lobbyists successfully suggested agenda items before meetings and requested readouts of official discussions. For example, a Feb. 14, 2025 email from CCIA noted the upcoming visit of South Korea's trade ministers and stated, "I hope the issue we discussed can get on the agenda, and if possible, we could get a read-out of any digital-relevant discussions." In a separate thread with Amazon



regarding Korea's "trade barriers," the USTR's Senior Director for Information and Communication Technology Services and Digital Trade noted she would be leaving for South Korea on February 26, so moved the meeting up to February 25 to make sure they could discuss relevant issues before she left.

Emails indicate that industry groups provided briefing materials, backgrounders, and "non-papers" — informal documents without attribution. USTR did not just receive information passively from these groups, but actively sought it as well. USTR staff requested industry position papers shortly after meeting foreign officials to use in their push against foreign digital regulations. There is evidence that at least twice, a USTR staffer requested an industry group's communications with foreign regulators, giving assurances to the industry group that USTR was pressuring the foreign government on their behalf.

The result is a U.S. government and Big Tech collaboration to push back against digital economy regulations across the world — in Korea and elsewhere.

What's the bottom line?

Coupang's investors appear willing to weaponise every tool at their disposal to stave off regulatory oversight of their company, irrespective of the harm caused by its business practices to Korean consumers and workers. This follows a trend of Big Tech companies using [trade policy](#) to attack public interest digital regulations around the world. And unfortunately, they appear to have found willing allies in the Trump administration and some in the U.S. Congress.

The Trump administration has actively used trade policy to coerce countries to implement policies favorable to U.S.-based multinational companies like Coupang. Instead of attacking other countries' modern data protection and competition laws, U.S. policymakers should focus on implementing and enforcing regulations domestically to hold Big Tech companies accountable. U.S. lawmakers should also be aware of the inclusion of provisions in trade agreements that could limit their ability to regulate the technology ecosystem.

