KEY THREATS TO DIGITAL TRADE 2023

South Korea

The United States and South Korea have a longstanding economic relationship underpinned by the United States-Korea Free Trade Agreement (KORUS), originally signed in 2007 and most recently updated in 2018. The U.S. and Korea are also partners in other regional and multilateral fora, including the WTO, OECD, APEC, and the Indo-Pacific Economic Framework (IPEF).

Strong trade and investment ties are an essential component of the U.S.- Korea Alliance, which has become ever more important in view of changing geopolitical realities. Digital services drive U.S. exports in this mutually beneficial relationship. **The United States generated $12.12 billion in exports of digitally-enabled services to South Korea in 2020, representing 68% of all U.S. services exports to South Korea**. The United States ran an $8.75 billion surplus in bilateral trade in digital services in 2020, compared to the overall deficit of $16.8 billion that the United States holds with bilateral trade in goods and services with Korea. Korea's profile reflects an enormous growth potential of the online services sector in the country—98% of the country uses the internet.

However, the digital regulatory environment in Korea has made it increasingly challenging for U.S. businesses to operate on a level playing field. Several policies pursued or already enacted by Korea's government have established barriers to U.S. digital exports and threatened the internet ecosystem:

1

Korea has established several restrictive data policies that hinder the provision of online services and cloud services from U.S. and foreign suppliers in the country. Unreasonably stringent technical requirements for cloud services providers—that appear designed to keep foreign competitors out of the Korean market—remain in effect and proposed amendments have failed to address their restrictive impact. Further, Korea has imposed several requirements that effectively restrict companies from exporting geolocation data—leaving international firms providing mapping and other location-based internet-enabled services at a significant competitive disadvantage.

2

Korea has continued to pursue obligations for foreign online services suppliers to pay internet service providers for the traffic generated by users of internet-enabled services. The adoption of such "sender-party-pays" policies would harm the very foundation of the open internet, extract large sums of money from foreign suppliers to redistribute to local telecommunications behemoths, and harm the provision of online content that relies on internet-enabled services.

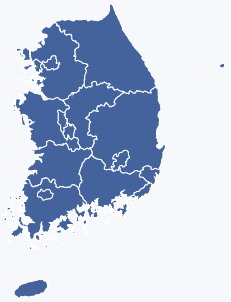
3

Korea has targeted U.S. companies for disproportionate enforcement from agencies such as the Korea Communications Commission, the Korea Fair Trade Commission, and Personal Information Protection Commission, and use their broad authorities and enforcement powers to benefit Korean companies at the expense of U.S. competitors or narrowly enforce against U.S. companies despite similar business practices by their Korean competitors.

CCIA identified **9** digital trade barriers in South Korea

6 policies have been enacted

3 are in development



Restrictions on Cross-Border Data Flows & Data & Infrastructure Localization Mandates — 4

Telecommunications-Related — 3

Other Trade Barriers — 2

ex: Amendments to the Telecommunication Business Act on Mobile Application Marketplaces, Proposed Artificial Intelligence Bill

The following sections profile the most problematic policies that concern the technology industry in Korea:

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates Affecting Digital and Cloud Services

US cloud service providers have been effectively shut out of Korea's public sector cloud market for years, due to requirements of the **Cloud Security Assurance Program** (CSAP) certificate that made it technically infeasible for US cloud providers with globally distributed networks to comply. The requirements included physical isolation of the cloud facilities for government workloads, Korea-specific security certifications and encryption algorithms that preclude use of internationally-standardized solutions, and unreasonable personnel and resource localization requirements.

The Yoon Administration recently made limited progress by introducing a tiered certification system based on data sensitivity classification (low, medium, and high), and relaxing requirements for "low" sensitivity public sector IT systems (which only contain public data and no personal information).

While burdensome requirements at the low tier remain (e.g., with respect to encryption), these changes have opened up a small portion of the public sector market to global CSPs, by allowing logical versus physical separation of data for this category. This key burden remains for medium and high-tier systems, which require the use of physical infrastructure separate from public cloud offerings. While recent advancements in AI technology are expected to benefit the Moderate tier of the public sector the most, their ability to utilize the most advanced global AI services may be significantly hindered by physical separation requirements. Given Korea's interest in developing its AI capability, allowing for logical separation in the Moderate tier, and alignment with international standards, should be a priority.

Also key to a more open market is a more open and transparent policy dialogue involving the National Intelligence Service (NIS), which has played a major role in cloud computing regulation, and creation of its independent National Cloud Computing Security Guide. The NIS Guidelines set stricter cybersecurity requirements than the CSAP guidelines, as well as other cybersecurity validation programs that impact CSAP, including by requiring that cloud facilities, equipment and personnel be under the exclusive legal jurisdiction of Korea. Therefore, reform of these Guidelines to allow for U.S supplier participation in the Moderate tier, and NIS's increased involvement in policy discussions is crucial for ensuring more secure and reliable public services through the cloud.

Korea's **Personal Information Protection Act of 2011** has always imposed stringent requirements on the transfer of personal data outside Korea, requiring online service providers to provide customers with extensive information about the data transfer, such as the destination of the data, the third party's planned use for the data, and the duration of retention. However, less stringent requirements apply to data transfers to third parties within Korea, which "effectively privilege Korean over foreign suppliers in any data-intensive sector without materially contributing to privacy protection," as USTR has highlighted.

A recent **amendment to the Personal Information Protection Act** that takes effect September 14 provides Korea's Personal Information Protection Commission ("PIPC") the authority to impose fines based on global, rather than local revenue. Since most Korean firms subject to this law have little foreign presence, such penalties disproportionately affect foreign (and mainly U.S.) suppliers, subjecting them to significantly higher financial risk than their local competitors.

This amended law also grants the PIPC the authority to order the suspension of cross-border transfer of personal data based on a generalized risk of breaching privacy protections, absent evidence of specific violations. Such arbitrary authority could affect legitimate personal data transfer by U.S. companies to their U.S. headquarters, jeopardizing significant cross-border trade between Korea and the United States.

Korea's **restrictions on the export of map data** continue to disadvantage foreign providers that use such data for services offered in Korea. Foreign-based services providers that offer apps and services that rely on map-based functions—such as traffic updates and navigation directions—are unable to fairly compete against their Korean rivals that generally do not rely on foreign data processing centers in the same way that international suppliers do and therefore do not need to export map data. Korea is the only significant market in the world that restricts the export of map data in this manner.

Exporting map data requires approval from the Korean government. To date, Korea has never approved the exporting of map data, despite numerous applications by international suppliers. U.S. stakeholders have reported that Korean officials have stated that export approval is dependent on an obligation to blur certain integrated satellite imagery of the country. However, such imagery is not managed by the Korean government (and therefore not subject to any approval of map data export) and is readily viewable on foreign mapping services available outside of the country. Despite Korean officials' stated interest in restricting the availability of high-resolution commercial satellite imagery of Korea abroad, the government has no tangible mechanisms to enforce such a policy since most imagery is produced and distributed from outside of Korea. It is unclear how restricting the availability and denying the export of such data for foreign suppliers would address the general security concern, since high-resolution imagery, including for Korea, is widely available as a stand-alone commercial product (and is often available free of charge), and offered by over a dozen different suppliers.

Network Usage Fees

Seven proposals have been made by the Korean National Assembly to mandate **"network use fee"** payments by certain content providers over the past two years. This is at times justified by an argument that network fees will help fund the costs of extending and adding capacity to local broadband markets, but would likely distort investment incentives and lead to discriminatory treatment of content and application providers. This follows years of conflict between U.S. content providers operating in the region and local telecommunication providers.

These proposals have been consolidated into the seventh piece of legislation on this matter, introduced by Rep. Young-chan Yoon, called the **"Netflix Free Ride Prevention Act"** on September 8, 2022. The legislation would effectively mandate foreign content access providers—namely U.S. firms such as Google, Meta, and Netflix—to enter into paid contracts with internet service providers for the content demanded by ISPs' customers. The bill would directly undermine long-standing global norms and procedures that serve as the foundation of the internet ecosystem and would likely violate Korea's trade obligations to the U.S. by targeting U.S. content providers and requiring contracts and extractionary fees for any company meeting arbitrary data transfer thresholds. In addition, the bill would have a detrimental impact on the domestic content industry by increasing the cost for users to access content and inhibit the overseas expansion of K-content. Korea's existing Sending Party Network Pays (SPNP) model, adopted in 2016 and applicable to ISPs operating in Korea, demonstrates that these concerns are not merely speculative. Multiple studies have found that Korea's SPNP model has led to higher transit prices, higher latency, and high regulatory costs.

The legislation would put South Korea in danger of violating several provisions of their Free Trade Agreement with the United States, including KORUS Article 14.2 (Access and Use); KORUS Article 14.5 (Competitive Safeguards); and KORUS Article 15.7.

Amendments to the Telecommunication Business Act on Mobile Application Marketplaces

In August 2021, the Korean National Assembly passed legislation that requires **mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself.** The scope of the law effectively creates a ban on a predominately used U.S. model, at the exclusion of local equivalents. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law. The targeting of U.S. firms could conflict with Korea's trade commitments under the Korea-U.S. Free Trade Agreement, as well as commitments under Article XVII (National Treatment) of the WTO General Agreement on Trade in Services (GATS).

The rules banning app store operators from requiring "specific payment methods" were approved by the Korea Communications Commission on March 8, 2022. The agency announced on August 16, 2022, that it was investigating Google, Apple, and SK Group's OneStore over potential violations regarding in-app payments, with a specific warning to Google and Apple: "In addition, the KCC determined that if Google or Apple imposes discriminatory conditions on the payment method (third-party payment) provided by the app developer in an internal payment, or makes the usage process inconvenient, that act may constitute an act of forcing a specific payment method (own company payment)."

U.S. operators of application marketplaces are disincentivized to operate in a region where it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace. Industry reports inconsistent and opaque definitions and implementation procedures of the legislation by the KCC which has resulted in uncertainty for businesses operating or seeking to operate in Korea.

Further, the lack of sufficient deliberation and input from parties, both domestic and foreign, on the merits and possible implications of the bill including potential harmful effects on a nascent and thriving ecosystem that countless Korean developers utilize to reach a global market.

Targeted Enforcement on U.S. Companies

In September 2022, the Korean Personal Information Protection Commission (PIPC) levied more than $70M in fines against two US companies for alleged violations of the Personal Information Protection Act (PIPA). These are the biggest fines ever imposed by the PIPC, and were based on a **new interpretation of the law with no court or regulatory precedents** that the ad tech service provider, rather than the third party publishers (website or app operators), must obtain consent for the user's personal data for personalized ads on the publishers' sites and apps. It appears that PIPC narrowly and arbitrarily scoped their investigation to only impact 2 US companies, even though several domestic ad service providers also use behavioral data for personalized ads with variations.

Taking this narrow approach to enforcement held US companies to an unprecedented responsibility, and effectively absolved domestic ad service providers and third party publishers of their responsibility to obtain consent for using behavioral information for personalized ads. Given there was no clear standard established by regulatory authorities or court precedents in Korea, and no establishment of harm to the user, the PIPC could have first clearly set forth the standards to be complied with by business operators in the form of guidelines and recommend them to comply with such standards.

Artificial Intelligence Legislation

On Feb. 14, 2023, the National Assembly Science, ICT, Broadcasting and Communications Committee advanced the **"Law on Nurturing the AI Industry and Establishing a Trust Basis"**, after 12 different bills related to artificial intelligence have been introduced in the previous three years. While the bill does not discriminate based on nationality or size, it includes increased and unclear obligations on systems of AI determined to be "high-risk," including methods for detailing how an AI system reaches its final decision. The broad classification of what constitutes high-risk is comparable to that of the EU AI Act and could envelop more services than appropriate.

Data Center Legislation

In late 2022, in response to a fire a major data center, the National Assembly passed the amendments to the Broadcasting Communications Development Act ("BCDA"), the Telecommunications Business Act ("TBA"), and the Act on the Promotion of Information and Communications Network Utilization and Information Protection ("Network Act") to encourage **resiliency of data centers.** The legislation will enter into force in July 2023. Among the requirements of this law are extensive demands for data related to data center security that could jeopardize companies' cybersecurity and nondisclosure agreements, and making sensitive data related to infrastructure, security, and commercially sensitive trade secrets vulnerable to exposure.