DIGITAL TRADE ORDER AND CURRENT ISSUES

Professor: **AHN Dukgeun**
Classroom: **Building 140/R101**
Class Hour: **Tuesday 14:00-17:00**
Office Hour: **Tuesday 1:00-2:00** or **by appointment**
E-mail: **dahn@snu.ac.kr**

COURSE DESCRIPTION

Global trade orders have been substantially changed since "digital economy" has prevailed over traditional economy in many sectors. Most importantly, national boundaries that have been the foundation of most trade norms are now blurred or almost meaningless in the realm of digital economy. Thus application or implementation of traditional trade rules becomes very difficult – if not impossible – to embrace new technological development. Moreover, recent development of artificial intelligence (AI) has added additional layer of complexities to building digital trade order as well as digital economy.

This class will addresses those new features of digital trade to understand dramatically changing global trade systems and prepare the future of global trade system. Although this class does not formally require any prerequisite course, other trade classes dealing with core trade rules are strongly recommended.

The final assessment for the course will be based on a group term paper. Class participation and presentation will be favorably considered in your final grade up to 50%.

COURSE OUTLINE

P. van den Bossche & Werner Zdouc, "Law and Policy of the World Trade Organization" (5th ed. 2022) provides good basic explanation for key trade rules. Students with serious interest in a particular issue may want to refer to Petros Mavroidis, The Regulation of International Trade, V:I, II, & III. More reading materials listed in the syllabus will also supplement recent academic and practical developments.

Students in this course are also advised to regularly keep up current developments in international trade area. Useful sources include, *inter alia*, Inside US Trade (Site Licensed), Financial Times, and The Economist.

1. Historical Development of Global Trading System

- GATT
- WTO (+ GATS, TRIPS)
- Digital Trade Agreements

2. Global Trade in Reality

(1) Trend of Trade in Goods and Services

(2) Top 5 Export and Import Products

(3) Top 5 Trading Partners for major countries

- Data for digital trade?

3. Non-discrimination Principle

- Scope

- Non-discrimination for GATT, GATS, TRIPS and Digital Trade

4. Services Trade

- Audio-visual service v. Over-the-top (OTT) media service

. Digital Trade: Goods or Services?

- Digital "Product"

- US v. EU approach

5. Basic Principle for Digital Trade

- Data Free Flow

- Prohibition of Server Localization

- Privacy Protection

6. National Security Exception in Trade Rules

- James Bacchus, "The Black Hole of National Security: Striking the Right Balance for the National Security Exception in International Trade", CATO Policy Analysis No. 936.

- US CIT Joint Brief of Amici Curiae for V.O.S. Selections, Inc. v. Donald J. Trump (2025).

- Thomas A. Berry, Brent Skorup, and Charles Brandt, "Legal Brief: Even in Emergencies, the President Cannot Seize Congress's Tariff Powers", CATO (2025), <https://www.cato.org/blog/legal-brief-even-emergencies-president-cannot-seize-congresss-tariff-powers>

7. Cybersecurity: National Security, Economic Security or Business Security?

- Privacy Protection

- Export Control Regulation

Semiconductor Case of the US v. Rare Earth Case of China

- Investment Screening Rules of the US: CFIUS

8. Technical Barriers to Trade & Trade Facilitation Agreement

- Example: different release dates for Apple products, camera shutter sound, etc
- Certification process
- Mutual Recognition Agreement

9. Intellectual Property Protection for Digital Development

- Intellectual property by AI?

https://www.nytimes.com/2024/10/13/briefing/nobel-prize-artificial-intelligence.html

https://www.economist.com/science-and-technology/2024/10/10/ai-wins-big-at-the-nobels

https://www.japantimes.co.jp/business/2025/03/28/companies/chat-gpt-ghibli/

- Intellectual property for AI?

https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem

https://www.forbes.com/sites/douglaslaney/2025/02/11/copyright-or-copywrong-ais-intellectual-property-paradox/

https://www.dentons.com/en/insights/articles/2025/january/28/ai-and-intellectual-property-rights

https://www.oecd.org/en/publications/intellectual-property-issues-in-artificial-intelligence-trained-on-scraped-data_d5241a23-en.html

https://www.wipo.int/documents/d/frontier-technologies/docs-en-pdf-generative-ai-factsheet.pdf

10. AI Data Center and Energy Policy

- Datia & Lawrence, "Shaping the Future of Solar Power"
- AI and Energy (IEA, 2024)

- DJ Nordquist, "Embracing an All-of-the-Above Strategy for Energy and Economic Development" (Nov. 2024), Carnegie Endowment for International Peace <https://carnegieendowment.org/research/2024/10/nuclear-power-united-states-energy?lang=en>

- Nuclear Power in China (World Nuclear Association) <https://world-nuclear.org/information-library/country-profiles/countries-a-f/china-nuclear-power>

- Nuclear Power in Russia <https://world-nuclear.org/Information-Library/Country-Profiles/Countries-O-S/Russia-Nuclear-Power>

- Nuclear Power in USA <https://world-nuclear.org/information-library/country-profiles/countries-t-z/usa-nuclear-power>

11. Digital Trade in Reality: Cloud Security Assurance Program

[USTR 2025 National Trade Estimate Report]

(1) Korea

> The Cloud Security Assurance Program (CSAP) was created by the Korea Internet and Security Agency in 2016 and elevated from administrative guidance to a legal requirement through a March 2022 revision to the Cloud Computing Promotion Act. The CSAP, which applies to Korea's central, provincial, and local public sector with very limited exceptions, creates significant barriers to foreign cloud service providers (CSPs) seeking to sell to Korea's public sector. CSPs are required to create physically segregated facilities for exclusive use by government-owned customers, comply with data localization of cloud systems, create backup systems and data, and ensure that operations and management personnel of cloud service providers are located within the territory of Korea to obtain the low-tier certification. CSPs must also use only NIS- certified encryption algorithms (ARIA or SEED).
>
> The potential market from which U.S. providers are being excluded is large and growing. In August 2022, Korea began a review of the CSAP with a view to reform it in a way that would open market access possibilities for foreign service providers, indicating it would benchmark the U.S. Federal Risk and Authorization Management Program (FedRAMP). On January 19, 2023, Korea revised the Notification of the Security Certification for Cloud Computing Services to introduce a three-tiered scheme dividing all public networks into three risk tiers under the CSAP, which still creates significant barriers to U.S. CSPs seeking to sell to Korea's public sector. Only those CSPs that have at least the mid-tier CSAP certification can effectively participate in the government's digital transformation initiative. The United States raised this issue on May 16, 2024 and urged Korea to align its cloud security certification requirements with other internationally accepted standards. In September 2024, NIS announced it will waive the local encryption algorithm requirement up to the mid-tier CSAP certification.

https://seo.goover.ai/report/202412/go-public-report-ko-df0a7ad3-171e-43fb-922f-ccf8c9ab94c7-0-0.html

https://www.tandfonline.com/doi/full/10.1080/01402382.2025.2491962?src=exp-la#abstract

(2) EU

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 I'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.

12. Digital Trade in Reality: Google Map

[USTR 2025 National Trade Estimate Report]

> 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 locally- based 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.

13. Digital Trade in Reality: In-app Payment

https://www.reuters.com/sustainability/boards-policy-regulation/us-judge-rules-apple-violated-order-reform-app-store-2025-04-30/

https://digital-strategy.ec.europa.eu/en/news/commission-finds-apple-and-meta-breach-digital-markets-act

14. Digital Trade in Reality: Network Usage Fee

[USTR 2025 National Trade Estimate Report]

> Since 2021, a number of bills have been introduced in the National Assembly that would require foreign content providers to pay network usage fees to Korean Internet service providers (ISPs). Because some Korean ISPs are also themselves content providers, fees paid by U.S. content providers could benefit a Korean competitor. Furthermore, such a mandate could be anticompetitive by further strengthening Korea's ISP oligopoly of three major providers to the detriment of the content industry. The United States raised this issue with Korea on several occasions throughout 2024.

Annex.

[USTR 2025 National Trade Estimate Report]

EUROPEAN UNION

ELECTRONIC COMMERCE / DIGITAL TRADE BARRIERS

Digital Services Taxation

The United States and EU Member States are among the 137 member jurisdictions to have joined the October 8, 2021, OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitization of the Economy, which called for all Parties to commit to not introduce digital services taxes (DSTs) in the future. On October 21, 2021, the United States, under the prior Administration, joined Austria, France, Italy, Spain, and the United Kingdom (UK) in a joint statement "on a transitional approach to existing Unilateral Measures while implementing Pillar 1." According to the statement, DST liability that accrued to Austria, France, Italy, Spain, or the UK during a transitional period prior to the implementation of Pillar 1 would be creditable in defined circumstances against future corporate income tax liability due under Pillar 1. In return, Section 301 trade actions initiated during 2019 and 2020 on goods with respect to each of Austria, France, Italy, Spain, and the UK were not continued. The arrangement set out in the October 21, 2021, joint statement was extended to June 30, 2024.

On January 20, 2025 the United States issued a White House Memorandum titled "The Organization for Economic Co-Operation and Development (OECD) Global Tax Deal (Global Tax Deal)." The memorandum stated:

The Secretary of the Treasury and the Permanent Representative of the United States to the OECD shall notify the OECD that any commitments made by the prior administration on behalf of the United States with respect to the Global Tax Deal have no force of effect within the United States absent an act by the Congress adopting the relevant provisions of the Global Tax Deal.

On January 22, 2025, appropriate representatives of the Treasury Department provided notice to the Director of the Centre of Tax Policy and Administration at the OECD. On January 24, 2025, the U.S. Permanent Delegation to the OECD provided similar notice to the Secretary General of the OECD.

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 DMA authorizes the Commission to impose fines not exceeding 10 percent of the total annual turnover of a gatekeeper, and in case of repeat offenses 20 percent of total annual turnover, and provides the Commission with the power to adopt "delegated acts" for portions of the DMA, thereby granting the Commission expansive authority to adopt additional regulation.

While the Commission has broad authority to determine that any provider of one or more core platforms services is a "gatekeeper," and is therefore subject to the DMA's requirements, the DMA sets out that the Commission should designate as a "gatekeeper" any provider that: (1) provides a core platform services in at least three Member States and has an annual EEA turnover of €6.5 billion (approximately $7.7 billion) or more over the previous three years, or an average market capitalization of at least €65 billion (approximately $78 million); and (2) has had, for each of the last three financial years, 45 million monthly active end users established or located in the EU and more than 10,000 yearly active business users established in the EU. A company that meets the criteria to be designated a gatekeeper under the DMA has a two-month period in which to notify the Commission that it believes that it meets the criteria to be designated a gatekeeper. Following that notification, the Commission has 45 working days to decide on the company's gatekeeper designation. Once a provider has been designated as a gatekeeper, the provider will have six months to come into compliance with a number of obligations set out in Articles 5 and 6 of the DMA. The Commission designated the first set of "gatekeepers" in September 2023 and they were given six months to comply.

The DMA defines "core platform services" to include a broad swath of existing digital services, including online intermediation services, online search engines, online social networking services, video sharing platform services, number-independent interpersonal communications services, operating systems, cloud computing services, and advertising services (including networks, exchanges, and any other advertising intermediation services). The DMA provides the Commission with authority to add new services to the list of "core platform services."

The DMA gives the Commission broad authority to conduct market investigations to determine whether to designate a provider as a gatekeeper and whether a gatekeeper is in full compliance with obligations under the DMA. If the Commission determines that a gatekeeper has "systemically infringed" obligations in Articles 5 and 6 of the DMA and has "further strengthened or extended its gatekeeper position," the Commission may impose "any behavioral or structural remedies" that are proportionate to the infringement.

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.

Artificial Intelligence (AI) Act

The EU AI Act entered into force in August 2024, with rules applying in a staggered manner between February 2025 and August 2027. The Act establishes a risk-based approach to regulating AI systems by identifying AI systems as minimal, limited, high, or unacceptable risks, and regulating accordingly, including through conformity assessment. The AI Act applies differentiated obligations to various actors, in an effort to include the AI systems' manufacturers, importers, and users. The Act's scope applies to services such as machine learning programs, translations programs, speech to text conversion, or forecasting and optimization programs. The Act employs the strictest requirements on applications deemed "high-risk", such as facial recognition technology, credit scoring, and critical infrastructure. AI systems deemed as "unacceptable risk" are banned.

The Act will be supplemented by Implementing Acts and standards to operationalize its requirements for general-purpose AI, foundation models and high-risk AI. The Commission launched a consultation on a Code of Practice for providers of general-purpose AI (AI systems designed to perform a broad range of tasks, such as large-language models), which is expected to be finalized by April 2025.

The AI Act will also require providers of general-purpose AI to disclose a "sufficiently detailed" summary of their model training data. The Commission is currently developing a template for these disclosures. If the template requires granular disclosure of training data, it may impinge on the IP, including trade secrets of model developers.

CEN and CENELEC, the European standardization bodies, have launched a dedicated technical committee (JTC 21) to develop harmonized standards that will support the implementation of the AI Act, including a framework for AI trustworthiness and standards for AI risk management and quality assurance. It remains unclear whether these standards will be consistent with existing ISO standards (*e.g.*, ISO 42001). Divergent standards would require U.S. firms to adapt to EU-specific requirements.

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.

In July 2016, the European Commission granted the United States an adequacy decision that applies to companies participating in the EU-U.S. Privacy Shield Framework. In July 2020, however, the CJEU issued a judgment in the Schrems II litigation that invalidated the Commission's decision. Although the CJEU's judgment upheld the overall validity of SCCs, it nonetheless imposed an affirmative obligation on entities using SCCs "to verify, on a case-by-case basis ... whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data production clauses ...." In January and February 2022, multiple European Data Protection Authorities issued rulings that certain websites transferring analytics data to the United States were in breach of the GDPR, based on the Schrems II judgment. On March 25, 2022, the United States and EU announced that they have agreed in principle on a new EU-U.S. Data Privacy Framework (DPF), which is designed to provide a new mechanism to comply with EU data protection requirements for the transfer of personal data from the European Union. In July 2023, the Commission granted the United States an adequacy decision for the DPF, and organizations that self-certify their compliance with the DPF principles started transferring personal data from the EU to the U.S. in reliance on the DPF without SSCs. As of December 31, 2024, there were two pending legal challenges in the CJEU against the DPF, one on administrative grounds and one on substantive issues.

Network Usage Fees

On May 2, 2022, the European Telecommunications Network Operators Association (ETNO) released a report urging the European Commission to adopt new regulation that would require large Internet-enabled service suppliers to pay network usage fees to European telecommunications network operators in order to recoup costs they claim telecommunications network operators bear due to carrying high-bandwidth content. On October 7, 2022, the Body of European Regulators for Electronic Communications (BEREC) adopted a report that concluded the ETNO proposal was unnecessary and "could be of significant harm to the Internet ecosystem." On February 23, 2023, the European Commission launched a public consultation on the EU's connectivity sector and telecommunications infrastructure. On May 19, 2023, the United States submitted formal comments to the European Commission raising concerns with mandating direct payments from content and application suppliers to telecommunications network operators. On October 10, 2023, the European Commission published the results of this consultation, concluding that no plan for network usage fees would proceed given the feedback from stakeholders. On February 21, 2024, the European Commission published a white paper entitled "How to Master Europe's Infrastructure Needs?". On September 17, 2024, President of the European Commission, in her mission letter to the Executive Vice- President-designate for Tech Sovereignty, Security and Democracy, charged her with work on developing a new "Digital Networks Act to help boost secure high-speed broadband, both fixed and wireless" and directed her to "incentivize and encourage investments in digital infrastructure, taking into account responses to the Commission's White Paper of February 2024."

Class Schedule

Class	Date	Topic
1	9/2	Historical Development of Global Trading System
2	9/9	Global Trade in Reality
3	9/16	Non-discrimination Principle
4	9/23	Services Trade
5	9/30	Basic Principle for Digital Trade
6	10/14	National Security Exception in Trade Rules
7	10/21	Cybersecurity: National Security, Economic Security or Business Security?
8	10/28	Technical Barriers to Trade & Trade Facilitation Agreement
9	11/4	Intellectual Property Protection for Digital Development
10	11/11	AI Data Center and Energy Policy
11	11/18	Digital Trade in Reality: Cloud Security Assurance Program
12	11/25	Digital Trade in Reality: Google Map
13	12/2	Digital Trade in Reality: In-app Payment
14	12/9	Digital Trade in Reality: Network Usage Fee
15	12/16	Final Exam