跨境電子商務與數位貿易發展學術研討會

國家安全考量與數位貿易談判

National Security Concerns and Digital Trade Negotiations

陳在方 教授兼所長

國立陽明交通大學

科技法律研究所

Agenda

- Defining Digital Trade
- Framing National Security in the Digital Age
- Leading Approaches: U.S., EU, and China
- WTO and the Joint Statement Initiative (JSI)
- Balancing Trade Liberalization with Security

National Security in the Digital Age

- Protecting critical infrastructure (telecommunications, energy grids).
- Safeguarding sensitive data (personal data, proprietary technology).
- Addressing cyber threats, espionage, and foreign surveillance.
- Ensuring data sovereignty and technological self-reliance.
- Preventing misinformation and propaganda.
- Recognizing the importance of artificial intelligence.

The EU Perspective

- Focus on data privacy and protection (GDPR).
- Cybersecurity measures for critical infrastructure and essential services.

China’s Perspective

- Strong emphasis on cybersecurity and broad definitions of national security.
- Data sovereignty: Strict data localization and review mechanisms; state control over data flows.
- Strong essential security exceptions.

The U.S. Perspective

Previous Approaches

- Liberalized data flows: Opposing data localization requirements and insisting on free flow of data.
- Encouraging cybersecurity cooperation and targeted export controls on sensitive tech.

Data Transfer: USMCA

> No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.

Location of Computing Facilities–U.S.-Japan Digital Trade Agreement

> Neither Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.

Source Code–U.S.-Japan Digital Trade Agreement

1. Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory.
2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of the other Party to preserve and make available the source code of software, or an algorithm expressed in that source code, for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.

Non-Discriminatory Treatment of Digital Products–U.S.-Japan Digital Trade Agreement

> Neither Party shall accord less favorable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of the other Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of the other Party, than it accords to other like digital products.

The Change of U.S. Positions in JSI Meeting (Oct 2023)

• US withdrew its proposals on data flows, data localization and source code in JSI. Non-discrimination treatment of digital products is also mentioned.

• Office of the U.S. Trade Representative spokesman Sam Michel:

> Many countries, including the United States, are examining their approaches to data and source code, and the impact of trade rules in these areas.
> In order to provide enough policy space for those debates to unfold, the United States has removed its support for proposals that might prejudice or hinder those domestic policy considerations.

IPEF, position on EU rules, digital trade barriers in annual National Trade Estimate.

Comparing Key Approaches

Similarities:

- Recognizing cybersecurity as essential.
- Protecting critical digital infrastructure.

Differences:

- U.S.: Market-oriented, fewer restrictions, promotes free flow of data*.
- EU: Privacy-centric, stringent data protection.
- China: State-led control, robust localization, and security-driven filters.

Key Takeaways

- Digital trade is integral to modern economic systems.
- National security concerns are increasingly shaping the terms of engagement.
- The concept of national security in digital trade is rapidly expanding, leading to the border use of essential security exception and a lower level of substantive obligations.