Implications of the Privacy Exception in the WTO Agreement on Electronic Commerce

Introduction

Participants in the World Trade Organization's (WTO) Joint Statement Initiative on E-Commerce (JSI) reached an agreement on issues related to digital trade on July 26, capping off a 5-year plurilateral negotiation involving 90 WTO members. This agreement, dubbed the "Agreement on Electronic Commerce" does not include all issues originally proposed (e.g. data-related rules), but the co-convenors (Australia, Japan, and Singapore) judged this package to be the best near-term outcome possible. Among the JSI members, Brazil, Colombia, El Salvador, Guatemala, Indonesia, Paraguay, Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu, Türkiye and the United States all declined to join the agreement.

The text includes several commercially-significant outcomes reflecting rules common in free trade agreements, with the most notable one being a permanent moratorium on customs duties on electronic transmissions.

Despite these policy wins, this draft includes a highly problematic exception that would allow countries to restrict cross-border data flows — and in turn, trade in services that rely on such flows—by invoking the concept of privacy. The exception is below:

> ***Article 25: Personal Data Protection Exception***
>
> *Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of that Party provides for instruments enabling transfers under conditions of general application[1] for the protection of the data transferred.*

This exception, proposed by the EU, is the current template the EU uses in trade negotiations to ensure that the data flow and localization rules it includes cannot be used to challenge any EU privacy-related measures (i.e., rendering data flow/localization provisions essentially effective only for non-personal data).

Since data flow rules were removed from this current JSI package following the United States' withdrawal of its support for such rules last fall, this exception is completely unnecessary, as none of the remaining provisions implicate privacy. However, embedding such a broad exception in an agreement both cements the EU policy goal of ensuring that privacy restrictions cannot be disciplined by trade rules and also renders any future addition of data flow rules so weak and easy to circumvent as to be practically meaningless.

[1] *For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases.* (Note: this footnote appears in the text of the agreement).

The EU will correctly argue that the exception is not completely self-judging: the obligation on a country imposing restrictions to nonetheless institute a transfer mechanism does ensure that there is a theoretical path to ensuring that data can flow. However, since the nature of that transfer mechanism is not specified, countries are free to impose any number of restrictions-–including restrictions so burdensome and discriminatory as to render cross-border transfers economically infeasible (particularly for SMEs). For example, the JSI exception would allow countries to pursue the following localization mandate or restrictions on the cross-border flow of data in the name of privacy:

- Any localization mandate tied a privacy or data protection measure, such as Russia's Federal Law No. 242-FZ (the 2014 Data Localization Law) that includes a "mirroring" requirement for companies to keep a copy of data in-country;
- Conditioning data flows to a particular jurisdiction on legal changes in the destination country (e.g., following the breakdown of the U.S.-EU Privacy Shield mechanism in 2020, EU-mandated changes to U.S. laws);
- A requirement for cross-border transfers to be subject to additional consent requirements (above what might be required domestically);
- A requirement for a company transferring data to post a bond to do so;
- A requirement for a cross-border data to be encrypted using national encryption ciphers, whose key must remain in the home territory; and
- A requirement for pre-transfer approval and post-transfer auditing.

Existing Regimes That Would Be Legitimized Under the Agreement

The following laws are all examples of the harmful approaches to data governance that would be justified under Article 25 of the WTO Agreement on Electronic Commerce. These laws harm free expression, legitimate commerce, and the integrity of the open internet. Privacy measures that could fall within the scope of a shielded transfer mechanism; and localization measures that could be similarly shielded. Even if not explicitly for privacy, localization measures could be construed as "protecting" the data.

Country	Law	Specific provision	Description of effect	Mandatory Local Storage of Data
China	Personal information Protection Law	Article 39 Article 40	Obligation to provide data subject with extensive information on recipient, and obtain consent for transfer. Obligation to store any personal information connected to critical infrastructure (not defined, but encompassing telecommunications, financial services, transportation) in China.	Cybersecurity Law of the People's Republic of China: Article 37: Obligation for any critical information infrastructure operator (definition) that gathers or produces personal information or important data

				during operations within the mainland territory of China shall store it within mainland China.
South Korea	Personal Information Protection Act	Article 17 Article 39-12	Personal information controller may transfer personal information of a subject to a third party when consent was obtained by the data subject or when working within the scope of Presidential decree. Applies Art. 17 guidelines; Can only transfer data overseas if the provider obtains users' consent or if the organization makes public the information that will be transferred, the country to which the information will be transferred, date and method of transfer, entity receiving the information, and purpose for using the information.	
Vietnam	Personal Data Protection Decree	Article 25 Articles 26-28	Obligation to complete Dossier in order to enact a cross-border data transfer, be ready for inspections, and notify and cooperate with the Ministry of Public Security of data transfer. Obligation to adhere to data protection standards.	Article 26 of Decree 53: Personal information of service users in Vietnam, data created by service users in Vietnam, and data on relationships of service users in Vietnam are subject to storage in Vietnam.

Saudi Arabia	Personal Data Protection Law	Article 29	One can transfer Personal Data outside the Kingdom if it is to achieve an obligation under an agreement in which the Kingdom is a part, to serve the interests of the Kingdom, perform an obligation to which the Data Subject is a party, or fulfill another purpose as set out in regulation.	
Turkey	Personal Data Protection Law	Article 9	Personal data shall not be transferred abroad without explicit consent of the data subject; without consent, data may be transferred if adequate protection is provided, on the existence of commitment for adequate protection in writing, or when necessary.	
Indonesia				Electronic System and Transaction Operations Law Article 20: Obligation to manage, process, and/or store electronic data within the territory of Indonesia unless the relevant storage technology is not available in Indonesia.