

USALI Perspectives

The US-Japan Digital Trade Agreement and “Data Free Flow with Trust”

Can the US lead without a uniform data privacy law?

By [David G. Litt](#) and [A. Reid Monroe-Sheridan](#)

Published February 3, 2022

In the area of data policy, the world falls into several camps. With the General Data Protection Regulation (GDPR), the European Union staked out its view of why and how data should be regulated and limited exports of data to countries that do not meet its standards. Likewise, despite China’s walled-off internet and unabashed surveillance state activities, the country’s new Personal Information Protection Law now offers its residents protection related to commercial use of data that is similar to GDPR in many

respects, including significant restrictions on data exports.

The United States, meanwhile, has long advocated global internet growth with minimal regulation. The US has opposed data localization requirements and taxes on data-based services. Its policy aligns with the interests of US-based global enterprises and the country’s strong free speech tradition, driven forward initially by optimism that free flow of data via the internet can be a positive force around the globe.

Where does Japan fit in this picture? Japan has deep commercial relationships with both China and the United States, its [top two export markets](#). However, Japan's fundamental national security alliance is with the United States. Japan also has important commercial and cultural relationships with the EU and other nations around the globe. In January 2019, shortly after the launch of GDPR and timed to coincide with a [new EU-Japan trade agreement](#), Japan became the first country in Asia to obtain a [declaration by the EU](#) that it provides an adequate level of data protection to allow transfer of data freely between the EU and Japan under GDPR. (In December 2021, the Republic of Korea became the second Asian jurisdiction to obtain such a declaration.)

The catchphrase of “Data Free Flow with Trust” (“DFFT”) was promoted by Japanese Prime Minister Shinzo Abe’s administration in the lead-up to the 2019 G20 Osaka summit, hosted by Japan. The DFFT concept made it into paragraph 11 [in the G20 Osaka Leaders’ Declaration](#), which affirms some basic principles:

11. Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection,

intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy. We will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development. We also reaffirm the importance of interface between trade and digital economy, and note the ongoing discussion under the Joint Statement Initiative on electronic commerce, and reaffirm the importance of the Work Programme on electronic commerce at the WTO.

This statement, though admittedly vague, is the closest thing we have to a shared understanding of what is meant by data free flow with trust. We think that in the context of DFFT, “trust” requires evaluating whether the legal protections for data in the transferee country are sufficient, without being overly burdensome, to ensure that the policy goals underlying the transferor country's data protection laws will not be undermined by the data transfer and cross-border enforcement regime. With

protections that are both sufficient and reasonable, and interoperability among legal regimes, the transferor nation can trust that its data management public policy goals will not be materially harmed by the flow of data to the transferee nation.

The United States and Japan are closely aligned in supporting DFFT. Indeed, the US-Japan Digital Free Trade Agreement (“DFTA”) was signed only a few months following the Osaka G20 summit, on October 7, 2019 and although it does not mention DFFT, clearly attempts to strike a balance between “free flow” and “trust” in a variety of fields.

The DFTA commits the parties to a variety of policies intended to promote digital trade by addressing both the sufficiency of legal protections for data as well as the risks of overregulation and inter-regime conflicts. In addition to eliminating customs duties on digital products and prohibiting discriminatory treatment of the other country’s digital products, the DFTA prohibits each country from restricting the electronic cross-border transfer of information. Importantly, the covered information includes personal information, which has been subject to increasingly stringent regulation in both the U.S. and Japan in recent years. Although the DFTA includes various exceptions for permitted restrictions on information transfer, the restrictions generally may

not be broader than necessary to achieve their public policy objectives. The parties also commit to maintain a legal framework protecting the personal information of users of digital trade and agree that these frameworks should be interoperable.

The US-Japan agreement also generally prohibits data localization requirements. This prohibition extends even to financial institutions, provided that ongoing and complete access to the financial institutions’ data is provided to the applicable governmental authorities. Similarly, both countries are prohibited in principle from forcing businesses to disclose software source code or cryptographic methods or keys used in commercial digital products as a condition of doing business in the country. In addition, the countries affirm their commitment to strengthening their cybersecurity capabilities.

Post-Abe, Japan has continued aggressively to push forward the concept of DFFT, including via the launch of a new Digital Agency. There is a flurry of activity to define and develop international standards with respect to data integrity, data protection, the recognition of electronic signatures and electronic original documents, to name just a few topics. Many of these efforts promote “trust” in a broad sense, not limited to cross-border transfers. Although they cannot address every underlying challenge of cross-border

enforcement of data protection laws, these efforts can help to create an environment in which cross-border transfers are not an obvious threat to data protection and privacy.

So where do Japan and the US go from here as they strive to implement the concept of DFFT and spread its use to other countries?

The United Kingdom, Australia, and Singapore, among other countries, are expected to enthusiastically support further development of DFFT. Singapore has already reached “[Digital Economy Agreements](#)” with Chile, New Zealand, Australia, Korea, and the United Kingdom, which align closely with the concept of DFFT. A US-UK free trade agreement, negotiations for which are stalled for unrelated reasons, is likely to include broad protections for DFFT. And the US Senate Foreign Relations Committee has [recently called upon](#) the Biden Administration to negotiate a broad Asia-Pacific digital trade agreement via APEC.

The most significant barrier to leadership by Japan and the US to further implement DFFT may prove to be the lack of a uniform, nationally applicable data privacy law in the United States, administered by a primary data privacy regulator. US data privacy rules are an unnecessarily complex patchwork of the laws of fifty states, with an overlay of federal rules

governing, for example, data related to health care, financial services, and children. The US framework becomes ever more complex as California, Virginia, Nevada, and other states pass and implement new laws in response to gaps in the current system. Moreover, according to the Court of Justice of the European Union in its 2020 [Schrems II](#) decision, the ability of the US government to access data in surveillance programs is broader than that of EU governments, especially as it pertains to non-US citizens/residents. The US has not obtained an adequacy declaration from the EU under the GDPR, nor could it likely do so under current law. This muddled situation is hardly a realization of the “interoperability of different frameworks” envisioned by the G20 Osaka Leaders’ Declaration.

A simple illustration can be seen under Japan’s Amended Act on Protection of Personal Information, which will come into effect on April 1, 2022. The act requires consent to transfer personal data to third parties outside Japan. Under a recently announced implementing regulation, in order for the consent to be effective, a business must disclose the country or region where the receiver of data is located and the steps taken by the receiver to protect data (especially any deviation from [the OECD privacy principles](#)), and also [must provide a](#)

description of the personal information protection system in such country or region. The Japanese government plans to help businesses comply by publishing its own summaries of privacy law in 31 countries and regions. These 31 jurisdictions include the USA (federal) as well as Illinois, California, and New York, but not the forty-seven other US states or the District of Columbia.

Compliance to transfer customer data from Japan to the US will not be impossible – as it is not from the EU to

the US despite *Schrems II* – but it will be more burdensome. The required disclosures may remind the world just how confusing the US data protection system is and how gridlocked the efforts to legislate in Washington, D.C. have become. The most valuable and transportable of all assets – data – is subject to a local patchwork of laws, different substantive standards and different remedies. This does not seem like a system that can respond quickly and intelligently to the challenges of DFFT.



David G. Litt is a professor at Keio University Law School in Tokyo, Japan, and registered foreign lawyer in Japan, Of Counsel to O'Melveny & Myers LLP.



A. Reid Monroe-Sheridan is an associate professor at Keio University Law School in Tokyo, Japan and registered foreign lawyer in Japan.

Suggested citation:

David G. Litt and A. Reid Monroe-Sheridan, “The US-Japan Digital Trade Agreement and “Data Free Flow with Trust,” in *USALI Perspectives*, 2, No. 13, Feb. 3, 2022, <https://usali.org/usali-perspectives-blog/the-us-japan-digital-trade-agreement-and-data-free-flow-with-trust>.

The views expressed in USALI Perspectives are those of the authors, and do not represent those of USALI or NYU.

This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

