KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

November 10, 2015

Privacy Law, Cross-Border Data Flows, and the Trans-Pacific Partnership Agreement: What Counsel Need to Know

Privacy law has become such a hot-button issue that it now finds its way into multilateral trade treaties like the Trans-Pacific Partnership Agreement (TPP or Agreement). On November 5, 2015, the U.S. Trade Representative released the text of the TPP, an agreement among the United States and 11 Asia-Pacific countries (Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam). The Agreement—which is now before Congress for a straight up or down vote—sets trade rules to open markets and promote jobs and economic growth in all of the signatory countries. The TPP does something else as well. In recognition of "the economic and social benefits of protecting the personal information of users of electronic commerce," Article 14.8 of the Agreement sets forth agreed-upon standards for protecting personal information.

Anatomy of the Privacy Provisions

Article 14 of the TPP addresses electronic commerce. It defines "personal information" expansively as "any information, including data, about an identified or identifiable natural person." Art. 14.1. Article 14.8 obligates the parties to the Agreement to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce" and, in so doing, "to take into account principles and guidelines of relevant international bodies." Art. 14.8.2.

In a footnote, the Agreement clarifies that this obligation can be met in a variety of ways, such as "by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy." Art. 14.8.2, n.6. Whatever legal regime a party selects for protecting personal information, the party "should encourage the development of mechanisms to promote compatibility between these different regimes." Art. 14.8.5. Moreover, absent a "legitimate public policy objective," the parties are obligated to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." Art. 14.11.

For more information, contact:

J. Michael Taylor
+ 1 202 626 2385
jmtaylor@kslaw.com

John A. Drennan
+ 1 202 626 9605
jdrennan@kslaw.com

Joseph Laroski
+ 1 202 626 2647
jlaroski@kslaw.com

Alexander K. Haas
+ 1 202 626 5502
ahaas@kslaw.com

Julie A. Stockton
+ 1 650 422 6818
jstockton@kslaw.com

King & Spalding
Silicon Valley
601 S. California Avenue
Palo Alto, California 94304
Tel: +1 650 422 6700
Fax: +1 650 422 6800

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

The Agreement additionally specifies actions related to data transfer and processing that the parties may *not* take. As relevant here, for example, it prohibits laws that require data localization (that is, mandating that companies' computer servers are resident in a country). *See* Art. 14.13.2 ("No 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.").

The EU's Contrasting Privacy Paradigm

To provide perspective on all of this, it is instructive to compare the TPP privacy regime with the privacy regime currently in the European Union. These regimes appear to be in tension. The TPP expressly endorses "laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy," but the European Court of Justice (ECJ) recently invalidated exactly such an arrangement when it found that the Safe Harbor Framework was an unlawful legal mechanism for transferring personal information from the EU to the United States. That mechanism involved participants voluntarily certifying that they treated personal information in a way is consistent with EU law, as well as authorized the U.S. Federal Trade Commission to enforce these voluntary undertakings.

Similarly, while the TPP proscribes data localization (with a notable exception for financial services), some European officials have suggested that in view of the ECJ decision, data localization is the *only* legal means for processing personal data in the EU. Hamburg's Commissioner for Data Privacy and Freedom of Information, Johannes Caspar, reportedly recently announced an investigation into data transfers from the EU to the United States by Google and Facebook. Caspar said that "[w]hoever wants to remain independent of the legal and political implications of the judgment [of the ECJ], should in particular consider to store personal data in the future only on servers within the European Union."

In short, recent changes in European privacy law provide that member states are not currently obligated to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person," as in the TPP. This provides a unique juxtaposition, because the European Commission and the United States are now negotiating a revised Safe Harbor—the so-called Safe Harbor 2.0. Privacy also remains a sticking point in the ongoing Transatlantic Trade and Investment Partnership (TTIP) negotiations.

Recommendations

Playing out on the world stage are contrasting approaches to privacy and international data transfers—the TPP's approach, which strongly encourages such transfers when personal privacy can be protected, and the EU's apparently more restrictive approach.

Companies involved in cross-border data transfers should pay careful attention. While it is possible that both approaches will continue to coexist, it is also possible that one or the other will achieve dominance (or that they will start to resemble one another more closely over time). Regulatory enforcement and litigation will inevitably follow close behind. To avoid being caught between conflicting privacy regimes, companies should get out ahead of this trend by assessing their data flows and their legal bases.