Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Latest Cross-Border Privacy Rules In Asia-Pacific

Law360, New York (September 8, 2015, 10:32 AM ET) --


Jeffrey L. Bleich Grant A. Davis-Denny

With the expected passage of the Trans-Pacific Partnership, U.S. cloud-based companies have recently refocused on opportunities in Asia. Four of the leading TPP partners in the Asia-Pacific region — Australia, Japan, New Zealand and Singapore — not surprisingly are also four of the most advanced in establishing regulatory rules for cross-border data flows. The good news is that these economies are moving to rationalize their regulations in a way that makes them more consistent; but the other news is that these countries are evolving toward more regulation rather than less. For example, New Zealand has adopted some EU-style restrictions, and Japan appears poised to significantly amend its privacy law. Other Asian economies may soon follow suit.

This article offers guidance to corporate counsel for U.S.-based software-as-a-service ("SaaS") companies, as they prepare to enter the rapidly growing economies of the Asia-Pacific region. In particular, it offers an overview of the cross-border data privacy frameworks in the region.

Challenges include the recent expansion of restrictions on cross-border data transfers in Asia-Pacific; opportunities include the alignment of standards among some leading nations, and a nascent Asia-Pacific Economic Cooperation-established system that could simplify compliance with data privacy standards. The situation is fluid, and so corporate counsel — particularly those whose businesses depend on the receipt of digital health, finance and other personal data — will need to pay close attention to regional developments in cross-border data privacy.

Australia

Last year, Australia enacted significant amendments to its Privacy Act, which now contains 13 Australian Privacy Principles ("APPs"). Most recently, the Australian information commissioner released guidance

for businesses on whether the APPs bar Australian companies from storing personal information in foreign clouds. His answer: “Generally, no.” Specifically, Australian information can be stored in foreign clouds in most sectors, but with conditions.

An Australian company that wants to disclose the personal information of Australians to a foreign business must take reasonable steps to ensure the foreign company does not breach the APPs. According to the information commissioner, reasonable steps generally mean an “enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs.”

There are two notable exceptions that can relieve foreign companies of this obligation to enter into a binding contract. For one, if the foreign business is itself subject to laws or a “binding scheme” that is “at least substantially similar” to the APPs’ approach to protecting information and Australian individuals have a means to enforce that protection, the business need not comply with the APPs. Alternatively, an Australian company can obtain customers’ informed consent to pass their information to a foreign business that does not have privacy controls that align to the APPs.

The APPs’ general rule does not apply equally across all sectors, however. For example, Australia has particularly restrictive legislation when it comes to health records; the country generally prohibits holding or taking medical records related to particular Australians outside of the country. Unlike other types of personal information, binding contracts, equivalent laws, and informed consent do not provide exceptions to Australia’s prohibition on exporting medical records.

Singapore

Singapore also saw key provisions of its Personal Data Protection Act (“PDPA”) go into effect in the past year. Like the Australian APPs, Singapore’s PDPA generally prohibits transferring personal data outside of Singapore unless the receiving overseas company provides assurances that it will comply with the PDPA standards. Specifically, foreign companies subject to legal obligations — i.e., contracts, laws, or binding corporate rules (in the latter case, for intracorporate group transfers only) — that are “comparable” to the protections under the Act may receive personal data from Singapore. As with Australian consumers, Singaporean data subjects may consent to the transfer of their data outside national borders.

But Singapore’s cross-border privacy rule is in some ways more friendly than Australia’s policy to the free movement of data. For example, Singapore’s Personal Data Protection Commission (“PDPC”) has issued guidance that cross-border transfers “necessary for the performance of a contract between the organization and the individual” data subject are deemed to have satisfied the comparable-protection standard, regardless of whether the foreign jurisdiction’s privacy laws are comparable to Singapore’s PDPA. An exception that has the potential to be even broader protects transfers “necessary for the … performance of a contract between” a Singaporean company and a foreign business “which a reasonable person would consider to be in the individual’s interest.” SaaS businesses hoping to receive data exports from Singapore should monitor how the PDPC interprets and applies these unique exceptions.

New Zealand

Unlike Australia and Singapore, which seem to be forging a new Asian-style approach, New Zealand has tended to look more toward European regulatory models. Indeed, in order to qualify for an adequacy

finding from the EU (i.e., a determination by EU regulators that New Zealand has data privacy standards that are sufficiently comparable to EU standards such that personal data can be transferred from the EU to New Zealand without additional contractual provisions or other measures), New Zealand adopted a unique cross-border data privacy rule.

New Zealand's privacy commissioner has authority to prohibit data that is imported into New Zealand from being exported if the commissioner is reasonably satisfied that (1) the receiving nation lacks "comparable safeguards" to those that exist in New Zealand; and (2) the transfer would contravene principles in the Organization for Economic Cooperation and Development's privacy guidelines. New Zealand's goal in implementing this import/export restriction was to show the EU that New Zealand could prohibit a European company from using New Zealand's EU adequacy status as a conduit for routing information to a third country not deemed by the EU to have adequate privacy controls.

Japan

Japan does not have specific restrictions on cross-border data transfers. But that may soon change. Japan's Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (a name that defies acronyms) released a policy position paper in 2014 that proposed requiring domestic companies holding personal data to impose contractual data privacy requirements on overseas recipients of such data. And in March 2015, Japan's cabinet submitted to the Diet legislation that would amend the Act on the Protection of Personal Information. While the amendments have not yet been finalized, they may require that foreign entities comply with contractual restrictions on data privacy or reside in a country certified as having restrictions that are equivalent to those in Japan.

Hong Kong

Hong Kong's status may offer some insight into how other rising economies in the region will react to the developing data privacy regimes in Asia. In 1995, Hong Kong adopted a law governing cross-border data transfers. A decade later, however, the law has not gone into effect. In December 2014, Hong Kong's Office of the Privacy Commissioner for Personal Data issued a 19-page guidance note on its cross-border data transfer law, a potential sign that Hong Kong may soon begin enforcing this aspect of its data privacy law.

Once in force, Hong Kong's data transfer restriction will prohibit transfers of data collected, held, processed or used in Hong Kong, or by a company with its principal place of business in Hong Kong, outside Hong Kong except in limited circumstances. Those circumstances include countries that have been whitelisted by the Hong Kong privacy commissioner, countries that the business has reasonable grounds for believing have laws that are "substantially similar to, or serve[] the same purposes as," Hong Kong's data protection law, and contractually enforceable agreements with the data recipient to ensure that the data will be protected consistent with Hong Kong's privacy standards.

While the standards may be similar to those in Australia and Singapore, the procedure for establishing them may be significantly more demanding. Importantly, the privacy commissioner has instructed that for a company to have a reasonable belief in the adequacy of another country's privacy laws, the belief must be objectively reasonable; must be supported by expert or professional advice, including the advice of legal professionals; and must be backed up by "evidence (for example, the legal advice sought) of the assessment which it relies upon."

APEC Cross-Border Privacy Rules System

While nations in the region have focused principally on requiring compliance with their own domestic privacy rules, there is a movement toward a common standard of privacy throughout APEC. In 2012, APEC adopted a system called the Cross Border Privacy Rules ("CBPR"). In brief, the CBPR establishes a voluntary certification system for complying with APEC's Privacy Framework.

Participation in the CBPR system is voluntary for both APEC member nations and for companies within those countries. Countries that opt to participate must designate an accountability agent and a privacy enforcement authority. The accountability agent has responsibility for assessing and certifying a company's compliance with the APEC Privacy Framework and only businesses based in the accountability agent's country (and such businesses' foreign and domestic subsidiaries) are eligible for certification by that accountability agent. The role of the privacy enforcement authority is to bring enforcement actions against companies that become CBPR certified but violate their own CBPR-certified privacy policies. The CBPR system applies only to data controllers, not data processors, although APEC is creating a separate but similar system called Privacy Recognition for Processors.

To date, participation rates in the CBPR system have been low at every level. Only four of the 21 APEC member countries have chosen to participate: the United States, Japan, Mexico and Canada. Of those four, only one has a qualified accountability agent: the United States, which has TRUSTe. And only about a dozen companies have obtained CBPR certification. The slow start, however, does not mean that the system is doomed to fail, only that it has yet to reach critical mass.

There is a first-mover problem in the CBPR system. For companies, the benefits of obtaining CBPR certification are limited. CBPR certification does not establish that a company complies with data privacy laws of APEC member countries. Nor have privacy enforcement authorities in countries like Australia deemed CBPR certification to be a "binding scheme" that is "substantially similar" to that country's domestic privacy principles such that CBPR certification would provide a safe harbor for data exports.

The main advantage of CBPR certification at this stage is marketing: A CBPR-certified company's customers and its business partners for whom data privacy is a salient issue are reassured that a third party has verified the company's compliance with the APEC Privacy Framework. Thus far, the market's verdict has been that this advantage is not enough to justify the costs of CBPR certification. This could change if more companies and countries signed up to participate and, perhaps more importantly, APEC member countries began accepting CBPR certification as evidence of a company's adherence to privacy standards that are "substantially similar" to their own domestic privacy principles.

Unfortunately, as long as participation rates remain low in the private sector, it is unlikely that privacy enforcement authorities and legislators in the APEC member nations will prioritize joining CBPR or treating CBPR certification as equivalent to compliance with national privacy standards. Thus, critical mass will be important before the real impact of CBPR can be known.

In sum, the leading nations in Asia seem to be moving toward more regulation regarding privacy of cross-border data, but also toward more reasonable and consistent regulation. While Australia has carved out health data as material that may not flow across borders in virtually any circumstance, no other nation in the region appears to be following that categorical approach. All nations seem to be looking toward a contract-based approach to ensuring that data recipients comply with local privacy laws. To the extent those local privacy laws can also be made more consistent, the regulatory environment for U.S.-based SaaS companies operating in Asia may become more promising, if still a bit complicated.

—By Jeffrey L. Bleich and Grant A. Davis-Denny, Munger Tolles & Olson LLP

Jeffrey Bleich is a partner in the firm's San Francisco office, former U.S. ambassador to Australia and former special counsel to President Obama. Grant Davis-Denny is a partner in the firm's Los Angeles office.