Data localisation in China and other APEC jurisdictions

In China, several sectoral regulations require data localisation, and the forthcoming Cybersecurity Law will introduce more obligations. Indonesia, Vietnam, Australia and Canada's British Columbia also have some form of localisation requirements. By **Scott Livingston** and **Graham Greenleaf**.

Data localisation provisions are becoming commonplace around the world. In many of these countries, local data protection laws may require that certain categories of data must be stored and processed on local servers within the country. Such provisions may require that some or all categories of personal data may only be stored and processed on local servers, or they make their export subject to conditions. Both types of provision may be called "data localisation".

Such laws are controversial. The proposed Trans-Pacific Partnership (TPP) treaty between some APEC member countries includes onerous requirements[1] on any Parties which have (or are considering) data localisation laws. These requirements are summarised below. Russia's recent data localisation requirements have also sparked considerable international concern and comment.[2] Whether they are consistent with Russia's obligations under Council of Europe Data Protection Convention 108 concerning free flow of personal data to other Convention parties adds another question, but does so in a treaty which does not have any Investor-State Dispute Resolution (ISDS) provisions, and so is unlikely to be resolved. Russia is also not likely to be a TPP party, so no test will arise from that direction.

The focus of this article is the data localisation requirements which are now emerging in China, an APEC member even though it has not proposed to become a party to the TPP. Examples of data localisation requirements from other APEC members – Indonesia, Vietnam, Canada and Australia – also illustrate the increased spread of such requirements, but without a comprehensive survey of all APEC members.

The TPP hurdles for localisation

The Trans-Pacific Partnership's anti-data-localisation provisions (TPP Article 14.13 – "Location of Computing Facilities")[3] follow a similar approach to its restrictions on data export provisions. First, formal acknowledgment is given to each Party's right to have its own "regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications". Then, a TPP Party is prohibited from requiring a service supplier from one of the TPP parties (a "covered person") "to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory". In other words, data localisation is *prima facie* banned. Then, the same "four-step-test" of justification for any exceptions is applied as was the case for data export limitations. Under some circumstances it is possible that a breach of the anti-localisation provisions by a Party could trigger entitlement to use of Investor-State Dispute Resolution (ISDS) provisions by affected companies. However, "computing facilities", for this Article, only include those "for commercial use," so there is considerable room for argument about when government-related services may be exempt from TPP requirements.

> In China, efforts to institute data localisation at the national level have begun to gather speed.

China's localisation requirements

In China, efforts to institute data localisation at the national level have begun to gather speed following increased attention to cybersecurity under the administration of President Xi Jinping.

These efforts take two forms. Historically, China has prohibited certain sensitive information from being transferred or stored overseas, such as state secrets or certain types of financial or health data. While not explicitly a data localization requirement, these restrictions have nevertheless had the effect of requiring local storage.

Recently, however, China has begun to affirmatively require data localization for a broader array of electronic data, a new and more assertive component of the nation's still evolving data privacy regime. These provisions have begun to crop up in a number of sectoral regulations and are soon to appear in China's first Cybersecurity Law, now expected to pass in late 2016.

Political factors: China's growing attention to data localization is one outgrowth of the Communist Party's increased focus on cybersecurity following the PRISM disclosures of Edward Snowden. These disclosures awakened Xi's administration to the importance of information security and alerted the ruling Party to the risks of having a national IT infrastructure still heavily dependent on foreign suppliers.

In the wake of Snowden, China realigned its Internet policymaking

registered repository operator, a registered portal operator or a registered contracted service provider that holds records for the purposes of the My Health Records system" (which includes a "personally controlled electronic health record") holding, taking or processing those records outside Australia. However, the System Operator can do so outside Australia provided the records do not include personal information or identifying information. The Health Department website says "Where My Health Records are created, they are stored in Australia. We will not disclose your health or other personal information overseas."[22] No other data localisation provisions in Australia are known.

Countries without major localisation requirements

APEC members not known to have any significant data localisation requirements are the Hong Kong Special Administrative Region, New Zealand, Taiwan and South Korea, as advised by local experts. This list is not comprehensive, as we have not considered other APEC members in the Americas, Singapore, Malaysia, Papua New Guinea and Brunei.

Conclusions

China's data localisation requirements are already extensive, but they are as yet sector-specific, both in relation to longer-standing regulations (banking and health) and new regulations (online publishing, ride sharing, Internet mapping and banking, finance and credit). A more sweeping approach to data localisation was eventually dropped from the 2015 Anti-Terrorism Law. Another version may soon be enacted in the Cybersecurity Law (nearing finalisation), which requires that "critical information infrastructure" providers store "citizens' personal information and important business data" within China unless their business requirements require overseas storage and they have passed a security assessment regarding such storage and transfer. Such a provision will have significant implications for many foreign businesses operating in China.

Among APEC jurisdictions, China is not alone in adopting data localisation requirements. As well as the obvious example of Russia's very sweeping law, they are found in at least Indonesia and Vietnam in very general forms, and in Canada and Australia in sector-specific forms.

AUTHORS

Scott Livingston, is a lawyer with SIPS Asia (Hong Kong)
Email: livingston.scottd@gmail.com
Graham Greenleaf is *PL&B's* Asia Pacific Editor and Professor of Law & Information Systems at UNSW Australia.

INFORMATION

Valuable information for this article has been provided by Michael Geist (Canada), Blair Stewart (NZ), Whon-il Park (Korea), Christian Schaefer (Vietnam), Fumio Shimpo (Japan), Clement Yongxi Chen (Hong Kong), Chen Hui-ling (Taiwan), Vanessa Halter (Australia) and Bernard Robertson (Australia). Andin Aditya Rahman has generously provided translations of key Indonesian provisions. All responsibility for content nevertheless remains with the authors.

EU e-Privacy revision on its way

The European Commission invited comments on the revision of the e-Privacy Directive by 5 July. It received 421 replies from stakeholders in all Member States as well as from stakeholders from outside the Union. The largest number of responses came from Germany (25.9%), UK (14.3%), Belgium (10.0%) and France (7.1%).

The majority of respondents thought that special privacy rules are needed for the electronic communications sector. But 76% of the citizens and civil society organisations that participated in the public consultation do not believe, or believe only to a limited extent, that the e-Privacy Directive has achieved its objectives.

It is understood that the Commission wants to broaden the scope of the legislation to include non-telcos which nevertheless provide similar services, such as instant messaging and Internet-voice-call services. Most respondents supported this overall aim.

The Commission is now carrying out an in-depth analysis of the replies to the public consultation, and will issue a full report later this year.

- *See ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive.*

US Cyber-Insurance Bill proposed

On 15 September, Representative Ed Perlmutter (D-CO) introduced H.R. 6032, entitled, "The Data Breach Insurance Act," law firm Arnall Golden Gregory reports.

The bill would provide a 15% tax credit to companies that purchase data breach insurance coverage and are in compliance with the National Institute for Standards and Technology (NIST) Cybersecurity Framework.

It is hoped that the Bill will incentivise companies to respond to the increasing risk of data breaches. The average cost of a data breach in the US is over $3.8 million, the Ponemon Institute says.

The Bill prescribes that the term "qualified data breach insurance" means coverage provided by an insurance company for expenses or losses in connection with the theft, loss, disclosure, inaccessibility, or manipulation, of data.

- *See www.congress.gov/bill/114th-congress/house-bill/6032/text?resultIndex=13*

