DATA LOCALISATION IN CHINA AND OTHER APEC JURISDICTIONS

SCOTT LIVINGSTON AND GRAHAM GREENLEAF

(2016) 143 *Privacy Laws & Business International Report*, 22---26, October 2016

[2017] *UNSWLRS* 11

UNSW Law
UNSW Sydney NSW 2052 Australia

Data localisation in China and other APEC jurisdictions

Scott Livingston and Graham Greenleaf*

(2016) 143 *Privacy Laws & Business International Report*, 22-26, October 2016

Contents

* Scott Livingston, is a lawyer with SIPS Asia (Hong Kong) email: livingston.scottd@gmail.com; Graham Greenleaf is Professor of Law & Information Systems, UNSW Australia. 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.

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.

China's localisation requirements

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

---

[1] Greenleaf, G 'The TPP Agreement: An anti-privacy treaty for most of APEC' (2015) 138 *Privacy Laws & Business International Report,* 1, 3-7; see also Greenleaf, G 'The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?' <http://ssrn.com/abstract=2732386> which considers other free trade agreements.

[2] Brian Zimbler and Ksenia Andreeva 'Russia's data localisation law affects foreign online businesses' (2016) 139 *Privacy Laws & Business International Report,* 26-7.

[3] For details, see Greenleaf 'The TPP Agreement' (above).

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 function, creating a Central Leading Group for Cybersecurity and Informatization chaired by President Xi, and consolidating coordinating work for internet policy in a new office dubbed the Cyberspace Administration of China.

From these new organs has emerged a strong focus on promoting cyber-sovereignty, the idea that national governments should have the right to supervise and control Internet content and infrastructure transmitted within their borders.[4] Along with calls at the domestic level for foreign technology to be "secure and controllable," China's new approach to the Internet is predicated on this theme of government control and oversight.

Central to this idea is the need for data localization, which China achieves through two means: prohibiting overseas transfers and requiring local storage.

Previous approaches: Prohibition on overseas transfers

Historically, Chinese laws and regulations have prohibited the overseas transfer or storage of certain types of sensitive information. Most notable is the restriction on overseas transfers of the broadly defined "State Secrets" contained in the PRC State Secrets Law.[5]

However, more industry specific provisions have begun to emerge in recent years to cover other types of sensitive data.

These recent efforts include:

- A 2011 *Notice to Urge Banking Financial Institutions to Protect Personal Information* that prohibited the overseas processing, storage or analysis of a Chinese citizen's personal financial data.[6]
- A 2013 voluntary national guideline that requires an individual's consent before the transfer of their personal information overseas.[7]

---

[4] See e.g., Scott Livingston, *Beijing Touts "Cyber-Sovereignty" in Internet Governance,* ChinaFile, Feb. 19, 2015, available at: https://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance

[55] The Law of the People's Republic of China on Guarding State Secrets [National People's Congress (NPC), 1989, revised 2010].

[6] Notice to Urge Banking Financial Institutions to Protect Personal Information [People's Bank of China, 2011].

- A 2014 *Measures for Administration of Population Health Information (For Trial Implementation)* that prohibits the storage on overseas storage of "population health information" (e.g., medical records) collected in China.[8]

Anti-terrorism law: Local data storage requirements dropped

More notable efforts to institute a nationwide data localization requirement were first revealed when the National People's Congress published a draft of the *PRC Anti-Terrorism Law* in November 2014. Under the draft law, "Internet content providers" ("ICPs," i.e., websites and apps)[9] would have been required to install government-accessible back doors in their products and turn over private encryption keys to public security authorities. In addition, the draft law would have required these entities to locate their servers in China and store all domestic user data on such local servers.

These requirements led to widespread criticism from governments and trade groups, with President Obama stating that he himself had raised concerns over the new law in meetings with President Xi Jinping.[10] Perhaps in response to such pressure, China removed or modified some of the more controversial requirements from the final passage of the *PRC Anti-Terrorism Law* in December 2015. In the final draft, the data localization requirement was removed in full while the encryption requirement was toned down to require ICPs to provide "technical support" to public security organs on request, rather than requiring the outright transfer of their encryption keys.

PRC cybersecurity law: Local data storage requirements proposed

However, as Chinese legislative drafters were removing these sensitive provisions from the *PRC Anti-Terrorism Law*, the National People's Congress was also debating and drafting a *PRC Cybersecurity Law* to "ensure network security, and preserve cyber sovereignty" that contained similar data localization requirements.

This draft law, now in its second reading, contains a data localization requirement for certain "critical information infrastructure" ("CII") providers (defined below) that requires such providers to 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 would constitute China's broadest data localization requirement to date. But the scope of who classifies as a CII provider remains unclear.

Under the law's first draft, CII was defined to include a number of public utility industries, such as energy, transportation or medical companies, as well as "networks and systems

---

[7] Information Security Technology – Guidelines for Personal Information Protection within Public and Commercial Services Information Systems [Standardization Administration of China & General Administration of Quality Supervision, Inspection and Quarantine, 2013].

[8] Administrative Measures for Population Health Information (For Trial Implementation) [National Health and Family Planning Commission, 2014].

[9] For further description of the scope of ICPs as well as the draft Anti-Terror Law itself, see: Scott Livingston, *Will China's Anti-Terror Law Mean the End of Privacy?*, ChinaFile, April 22, 2015, available at: https://www.chinafile.com/reporting-opinion/viewpoint/will-chinas-new-anti-terrorism-law-mean-end-privacy

[10] Ben Blanchard, *China Passes Controversial Anti-Terror Law*, Reuters, Dec. 28, 2015, available at: http://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228

owned or managed by network service providers with a large number of users."[11] This language would likely have placed the vast majority of Internet companies within its scope.

However, this language was removed in the law's second draft and replaced with a provision indicating that the State Council will promulgate a companion law to set out the specific scope and definition of CII providers.

This vaguer language could provide the authorities with the discretion to define CII on an ad hoc basis, until such time as the State Council provides more specific rules governing its scope. But as the law is still in draft form, it is also possible that the final draft of the new law will include more specific guidance.[12]

Other sectoral data localization regulations

Outside of the broadly sweeping data localization requirements found in the PRC Cybersecurity Law, data localization requirements have also begun to emerge in a number of new regulations targeting various industries. These include:

- Online Publishing: Effective March 10, 2016, the *Provisions on Administration of Online Publishing Services* requires online publishers to store their servers and storage equipment within China.
- Ride Sharing: Effective November 1, 2016, Article 27 of the *Interim Regulations for the Management of Network Appoint Taxi Services Operations* requires ride-sharing services like Didi Chuxing, to store all collected personal data and "produced business data" on PRC servers for at least two years.
- Internet Mapping: Effective January 1, 2016, the State Council issued the *Administrative Regulation of Maps*, which contained an entire chapter dedicated to "internet map services." This chapter requires a license (still heavily restricted for foreign enterprises) for online navigation and map databases, and requires that map data must be stored within China.
- Banking/Finance/Credit: A number of regulations have been promulgated that require local storage of credit information and personal financial information[13] and requiring both non-banking payment institutions and Chinese-invested banking institutions with e-banking services to keep their servers in China. Draft laws and guidelines have also been issued in the insurance and credit industries requiring the related storage of data within China.

Localisation in some other APEC jurisdictions

The range of data localisation requirements found in APEC countries – all potentially affected by the TPP's anti-localisation provision – is surprising varied in both source and content. The following examples are not intended to be comprehensive, but exemplify this diversity, and the difficult issues that countries acceding to the TPP may have to confront.

---

[11] See "China Releases Second Draft of Cybersecurity Law," Covington, July 12, 2016, available at: https://www.cov.com/-/media/files/corporate/publications/2016/07/china_release_second_draft_of_cybersecurity_law.pdf

[12] One factor that may explain this legislative uncertainty is the fact that as data localization policies have not been widely adopted worldwide, China cannot simply synthesize the best practices of other jurisdictions, as is their typical practice. Instead, Chinese regulators face the tough task of carving out new rules for emerging technologies, and doing so in a way that properly balances both national security concerns and the need to promote economic development. This is a difficult burden for any national legislature, and is arguably one reason, outside of foreign pressure, why drafts of the Anti-Terror and Cybersecurity Laws have encountered such legislative uncertainty.

[13] Notice of the People's Bank of China on Improving Work related to the Protection of Personal Financial

Indonesia

Indonesia's data localisation rules stem from Article 17 (2) of the Organization of Electronic Systems and Transactions Regulation (Government Regulation No. 82 of 2012), which states that electronic system administrators for public services (very broadly defined[14]) must locate their data centre and data recovery centre in Indonesia for purposes of law enforcement, protection, and enforcement of the state's sovereignty towards the data of its citizens. Any data related to public services are therefore required to be located in Indonesia, which includes, among other data, citizen administration, health services provided by public hospitals, and state-owned banks.

In addition to data related to public services, health data and information must be processed and stored domestically in a domestic data centre connected to the data centre managed by the Minister of Health.[15] However, health data and information may be processed overseas with the approval of the Minister of Health.

Claims have been made that these localisation requirements would damage Indonesia's economy,[16] but they give little consideration to the public interest justifications for the requirements.

Vietnam

Decree 72 of 2013[17] requires of enterprises that provide 'general websites' or 'social networking websites' (as distinct from 'specialised application websites' discussed below) to maintain at least one server system located in Vietnam that is subject to inspection from the authorities. Article 20.2 defines a general website as 'a website of a body, an organization or an enterprise providing general information quoting accurately official sources of information and specifying the name of the author or the name of the body of the official source of information and the time such information was posted or broadcast.' Social networks are defined under Article 3.22 as an 'information system providing network user communities with services of storage, provision, use, search, sharing and exchange of information with one another, including the services of personal website creation, forums, online chat, sharing of sounds or images and other similar forms of services.'

The storage requirement includes an obligation on general websites to store general information for at least 90 days from the time such information is posted on the site and to store logs of processed information for at least two years. For social networking websites, the requirement includes having to store information about accounts, time of log in and log out, IP

---

[14] Law No. 25 of 2009 regarding Public Services provides a very broad definition of 'public services' which covers: Procurement and distribution of goods, as well as the provision of services, conducted by government institutions, wholly or partially funded by the state budget or regional government budget; Procurement and distribution of goods, as well as the provision of services, by a business entity established wholly or partially by state assets or assets that are segregated from the state treasury; and Procurement and distribution of goods, as well as the provision of services, for purposes of fulfilling state missions. State missions are defined as policies to resolve specific issues, certain activities, or to achieve various goals that aim to benefit the general public. Examples include: 1) Appointment of PT (Persero) Pertamina to distribute fuel oil at the same price for retail throughout Indonesia, 2) Providing subsidies for fertilizers in order to encourage the production of farmers, 3) Policies to ensure the purchase price of grain through the determination of purchase price of grain that are purchased by the State Corporation of Logistics (Perum Badan Usaha Logistik), 4) Policies to safeguard food supply through determination of staple food prices, management of reserves and distribution of staple food, and 5) Public services provided by private entities, such as health services provided by private health facilities for the underprivileged, economy class air transportation (of which the prices' upper threshold are determined by the government), and incorporation of social service institutions.

[15] Government Regulation No. 46 of 2014 regarding Health Information Systems (China)

[16] Bert Verschelde 'The Impact of Data Localisation on Indonesia's Economy' ECIPE Bulletin No. 09/2014

[17] Decree No. 72/2013/ND-CP on Management, Provision and Use of Internet Services and Online Information (Vietnam)

addresses of users and logs of processed information for at least two years, and to provide personal information and private information of users related to terrorism, crimes or breaches of law upon request by competent State administrative authorities.

There is an exemption from these localization and data storage requirements for purely commercial websites which Decree 72 classifies as 'specialised application websites'. These are defined as 'the website of an agency, an organization or an enterprise which provides application services in the fields of telecommunications, information technology, broadcasting, television, commerce, finance, banking, culture, health care, education and other specialised fields without providing general information.'

The scope of Decree 72 is quite broad, in that it applies to 'domestic and foreign organizations and individuals engaged in or related to the management, provision and use of Internet services, online information, online electronic games, and ensuring information safety and security.' The interpretation of local experts[18] is that Decree 72 will apply to (i) business that are registered and operate physically from Vietnam; and will also apply to (ii) business located outside Vietnam but which offer services to Vietnamese users, or are in the Vietnamese language, or have a .vn address, or have some other connection with Vietnam. However, it is not so broad as to apply to any website accessible in Vietnam (e.g. search engines), but only where some form of cross border services are offered, particularly paid services that are performed (at least partially) in Vietnam. However applicability in such cases might be largely theoretical, because enforcing the regulation would be very difficult.

Canada (British Columbia)

Canada's British Columbia amended its *Freedom of Information and Protection of Privacy Act* (FOIPPA) in 2004, in response to the United States' *Patriot Act*.[19] The amendments extend requirements that apply to public bodies (defined broadly enough to include hospitals and schools) to 'service providers', defined as 'persons retained under a contract to perform services for a public body'. Among other obligations, public bodies and their service providers are required 'to ensure their storage of and all access to such personal information is restricted to locations within Canada'. As a result, 'a service provider located outside Canada can no longer store or access personal information unless it establishes facilities within Canada for this purpose',[20] and new or renewed contracts with (for example) US service providers have had to be amended to comply. The amendments then restrict the purposes for which a public body or service provider may disclose personal information outside Canada, essentially to purposes 'that are governmental in nature',[21] with broader purposes for disclosures within Canada being allowed.

Other Canadian provinces also have some restrictions relating to particular categories of information such as health data, for example Nova Scotia's *Personal Information International Disclosure Act* which requires medical data to be stored in Canada.

---

[18] These interpretations, and information in the preceding paragraphs, are provided by Christian Schaefer, Managing Partner, Asia Counsel, Ho Chi Minh City.

[19] Larry Munn 'British Columbia's Privacy Laws Amended In Response to the US Patriot Act', undated, Clark Wilson LLP website <http://www.cwilson.com/services/18-resource-centre/190-british-columbias-privacy-laws-amended-in-response-to-the-usa-patriot-act.html>

[20] Munn, ibid

[21] Munn, ibid

Australia

What was previously the 'personally controlled electronic health record system' (PCEHR) has been changed to the 'My Health Record system'. The *My Health Records Act 2012* s77 prohibits the 'System Operator, a 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.

Jurisdictions without significant localisation requirements

APEC members not known to have any significant data localisation requirements are the Hong Kong SAR, New Zealand, Taiwan and South Korea, as advised by local experts. This 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" ("CII") providers to 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.

[22] Australia, Department of Health <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/privacy-statement>