*University of New South Wales Law Research Series*

# PRC'S NEW DATA EXPORT RULES: 'ADEQUACY WITH CHINESE CHARACTERISTICS'?

**SCOTT LIVINGSTON AND GRAHAM GREENLEAF**

(2017) 147 *Privacy Laws & Business International Report* 9
[2017] *UNSWLRS* 69

UNSW Law
UNSW Sydney NSW 2052 Australia

**E:** unswlrs@unsw.edu.au
**W:** http://www.law.unsw.edu.au/research/faculty-publications
**AustLII:** http://www.austlii.edu.au/au/journals/UNSWLRS/
**SSRN:** http://www.ssrn.com/link/UNSW-LEG.html

# *PRC's new data export rules: 'Adequacy with Chinese characteristics'?*

Scott Livingston, Simone IP Services (SIPS)

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2017) 147 *Privacy Laws & Business International Report* 9-12

For over twenty years the European Union has defended its right to impose mandatory restrictions on exports of personal data from the EU, according primarily to its concept of 'adequacy' of protection in the export destination. These restrictions have been implemented in large part to ensure that each individual's fundamental rights and values, including most notably their right to privacy, are protected at all stages of the data lifespan.[1]

Recently, China has introduced a draft piece of legislation, the *Measures for the Security Assessment of Personal Information and Critical Data Leaving the Country (Draft for Public Comment)* ('Draft Security Measures'), that sets its own limits on data exports by covered parties. This legislation is intended as an implementing regulation for the recently released *PRC Cybersecurity Law* ("Cybersecurity Law"), which also contains a data localization provision requiring certain "Key Information Infrastructure Operators" ("KIIOs")[2] to store on PRC servers all personal and "important" data collected through their China operations.[3]

These new measures reflect a general upsurge in data localization measures occurring throughout the world,[4] and demonstrate a uniquely Chinese take on data export restrictions, one encompassing not just an individual's personal right to privacy, as in the EU, but also China's recent adoption of the principle of cyber-sovereignty -- the right for all countries to have jurisdiction and control over data flows occurring within their borders.

This approach has raised concern for foreign companies operating in China over fears that the laws may be used to require them to turn over sensitive data or IP to state authorities upon request. And, indeed, it's likely that these new measures were

[1] Directive 95/46/EC, Article 25

[2] These KIIO are sometimes referred to as "Critical Information infrastructure Operators" depending on how the first term (*guanjian)* is translated.

[3] Though less relevant to our present discussion, we note that our previous analysis of the *Cybersecurity Law* assessed it as including the most comprehensive and broadly applicable set of data privacy principles yet enacted in China, and close to meeting the basic international standards for a data privacy law. Greenleaf, G and Livingston, S 'China's Cybersecurity Law – also a data privacy law?' (2016) 144 *Privacy Laws & Business International Report*, 1-7; Greenleaf, G 'Global data privacy laws 2017: 120 national data privacy laws now include Indonesia and Turkey' (2017) 145 *Privacy Laws & Business International Report*, 10-13, concluding that China's law still falls short in a number of respects.

[4] S. Livingston and G. Greenleaf 'Data localisation in China and other APEC jurisdictions' (2016) 143 *Privacy Laws & Business International Report,* 22-26

motivated in part by China's own experience in having requests for data to foreign companies refused on the basis that the requested data was not stored in China.

In this article we detail the progressive implementation of China's data localization / data export measures through further examination of the Cybersecurity Law and the Draft Security Measures, and conclude with some general observations about the relationship between China's approach and the EU's 'adequacy' approach to data exports.

While much of our discussion herein will be focused on the specifics of these provisions and how they may encumber foreign businesses operating in China, we should also note the Chinese government's growing recognition of an individual's right to privacy, as demonstrated most recently with its identification of the "right to privacy" as a specific individual right in the latest version of the *General Provisions of the Civil Law* promulgated by the National People's Conference on March 15, 2017. While obvious barriers remain before these general provisions are fully realized in practice, the recognition and codification of the right to privacy here is at least a step in the right direction.

**Data Localization in the Draft Counter-Terrorism Law**

China first hinted at introducing data localization measures with the release of the draft *PRC Counter-Terrorism Law (Draft for Public Comment)* in November 2014. Under that draft's Article 15, companies providing "telecommunications or internet services within the borders of the People's Republic of China" would have been required to locate their related servers and domestic user data inside China.[5]

This provision was significant because, while China had long restricted data exports for certain types of sensitive data, such as state secrets or medical or financial records, it had not applied a data export or data localization requirement to any specific class of actors. The provisions found in the draft law were therefore seen as creating a far broader data localization requirement than had previously been found in Chinese law and one of the first of its type globally. While this provision did not make it into the final version of the now-promulgated *PRC Counter-Terrorism Law*, it nevertheless indicated that Chinese regulators had data localization squarely in their sites, and suggested that similar provisions would be forthcoming, ideally in less controversial legislation.

After the release of the draft Counter-Terrorism Law, "many Chinese and foreign companies voluntarily [had began] to plan for data localization in anticipation of stricter requirements to come."[6] It therefore came as little surprise when a draft form of the *PRC Cybersecurity Law* was released in July 2015 containing a similar data localization requirement for the so-called KIIOs. These requirements were made official in November 7, 2016 with the official promulgation of the *PRC Cybersecurity Law* by the Standing Committee of the National People's Congress. The law took effect on June 1, 2017.

[5] The reference to "internet services" here does not mean internet access services (as the term "Internet Service Providers" is used in the West) but rather services accessible on the internet, like websites.

[6] Sacks, Samm. "China's Cybersecurity Law Takes Effect: What to Expect." Lawfare Blog. 1 June 2016, <https://lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect>.

## Data Localization under the PRC Cybersecurity Law

Article 37 of the Cybersecurity Law requires KIIOs to store on local servers all personal information and "important data" collected or processed through their operations in China.[7] This data may not be transferred overseas unless such transfer is necessary for a "critical business purpose" and only following a government-defined security review.

Which entities are KIIOs remains vague. Within the law, KIIOs are defined to include any company involved with certain public-facing sectors such as 'public communications, information services, energy, transport, water conservancy, finance, public services, and electronic government, etc.' or any information infrastructure whose destruction or data leakage may cause harm to China's national or economic security.

Article 37 received considerable criticism following its publication for its vague definition of KIIOs and for its data localization requirement. This criticism was heightened following the April 2017 public release of the first version of the Draft Security Measures, which contained language expanding these data localization requirements to cover "network operators." another ill-defined and possibly broad reaching category.

Perhaps in response to these concerns, a second version of the Draft Security Measures was privately circulated in May 2017, which dropped the controversial data localization expansion and gave network operators until December 31, 2018 to comply with the data export provisions.[8]

It remains unclear if these provisions will be included in the final draft. Although the Draft Security Measures, along with several other implementing regulations, were meant to have been made effective concurrent with the Cybersecurity Law on June 1, they have yet to be officially promulgated, nor is there any indication that a final version is imminent. The Cyberspace Administration of China (CAC) has only said that implementation regulations will be brought in within a year of the law's commencement, but in the interim companies should observer the Cybersecurity Law.[9] The May draft is at present the only indication of what the final Measures may contain, but it appears that these items are still being negotiated by industry stakeholders both foreign and domestic.

## Expanded data export restrictions, but not localisation requirements

The Draft Security Measures are principally important for how they affect the cross-border data export of 'network operators' in China. Under Article 2, the proposed measures would apply to all network operators seeking to export overseas personal information and "important data" collected and generated in the course of their operations within China.

---

[7] Under a set of draft standards released on May 27, 2017, "important data" is defined as "Data that has a close relation with national security, economic development, and the public interest." This definition is then clarified through an extensive listing of potential important data in various sectors. See *Information Security Guidelines – Guidelines for Data Cross-Border Transfer Security Assessment (Draft)*. <http://www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf>.

[8] All quotations in this article refer to the May version of the Draft Security Measures, unless referred to otherwise.

[9] Teh, K and Kwok, P 'The Cyberspace Administration of China Clarifies the Cybersecurity Law' Dechert LLP, 1 June 2017 <https://info.dechert.com/10/8780/june-2017/the-cyberspace-administration-of-china-clarifies-the-cybersecurity-law.asp?sid=a37fd2ea-fea1-4a8f-a452-ad328dab2d68>

"Network operators" are defined in Article 15 as referring to "network owners, administrators, and network service providers", the same definition as in Article 76(3) of the Cybersecurity Law. The included term "network service providers" is not clearly defined under Chinese law and could be read broadly to encompass not only technology/online companies but also any company that uses its own IT networks or infrastructure.

In the previous (April) draft, the security reviews also appear to be extended by what was then Article 16 to apply to all 'other individuals or organizations that collect and process personal information and important/critical business data within the borders of the PRC'. This incredibly broad expansion has appeared to have been removed from the May draft of the Draft Security Measures.

### *Security assessments necessary for overseas transfers*

In most cases network operators are permitted to self-assess the cross-border transfer based on the 'type, volume and sensitivity' of the data (Article 6). Network operators are then instructed to reassess the security of the transfer whenever there is a "substantial change in the purpose, scope, type or volume of the cross-border transfer of data, or where there the data recipient is changed or has experienced a significant security incident."

In any of the above circumstances, the network operator is required to submit a report to the relevant industry regulator, and then entrust them to conduct a security review, if any of three defined situations apply:

- The data aggregates or contains the personal information of more than 500,000 individuals;[10]
- The data contains information on certain matters related to national security (e.g., nuclear facilities, population and health records or megaproject activities) or cybersecurity-related information such as security vulnerabilities or specific security measures of key information infrastructure;
- 'Other information likely to affect national security and societal and public interests'.

The draft's reliance on individual industry regulators to carry out the security assessments raises a fear that these security reviews may be applied unevenly across industries, thus potentially posing further hurdles for companies whose products or services straddle different sectors.

### *Factors involved in a security assessment*

Article 8 of the Draft Security Measures provides that a security assessment of a cross-border transfer of data (by either a network operator or an industry regulator) should focus on the following matters:

(1) the legitimacy, propriety and necessity for the cross-border transfer;
(2) the personal information involved, including the volume, scope, type, and sensitivity of the data, and whether the data subject has consented;
(3) the important data involved, including its volume, scope and type;
(4) the security protection capabilities of and measures taken by the data recipient, and the environment of the nation and region where the data recipient is located;

[10] The April 2017 draft of the Draft Security Measures included an additional category in instances where the volume of the data exceeded 1,000 GB. This was removed in the May 2017 draft.

(5) the levels of risks of data being leaked, damaged, tampered with, or misused after the cross-border transfer or subsequent retransfer;
(6) the risks to nationals security, social and public interest, as well as lawful interests of individuals.

While there is no specific mention of the level of legal protection provided to personal information in the country of the recipient, aspects of this could be taken into account under items (4), (5) and (6), all of which can be read as impliedly referring to a range of factors which are normally addressed by the data privacy laws of the receiving country, such as appropriate security measures, protection of the accuracy and completeness of information, limiting use and disclosure to the purposes for which the information was collected, and individual rights of access, correction and blocking. The 'environment' of the recipient nation may refer to the extent of legal protections, but this is speculative. All of these factors are relevant to what is taken into account in EU 'adequacy' assessments.

In the previous (April) draft, item (4) mentioned 'the cybersecurity environment of the nation and region where the data recipient is located' , and item (6) referred to 'risks posed by … offshore aggregation of data in relation to … the lawful interests of individuals.'

### *Mandatory blocking of some overseas transfers*

Article 9 of the Draft Security Measures sets out five conditions that would prohibit the transfer of data outside of China:

1) The cross-border transfer is in violation of relevant laws, regulations or rules;
2) The data subject has not consented to the cross-border transfer of the information;
3) The cross-border transfer will damage public and national interests;
4) The cross-border transfer will endanger the security of [any of a very wide range of national security interests]; or
5) Other situations where the CAC, Ministry of Public Security and Ministry of State Security have determined that no overseas transfer shall take place.

In these situations, there is effectively mandatory data localisation: the data must stay in China.

Each of these conditions, other than data subject consent, involves some element of discretionary decision-making, because these determinations are made by each industry regulator, with the overall guidance of the CAC (Art. 5). This gives rise to the possibility that certain data may be deemed a national security risk by one regulator but not another, again raising concerns that these provisions could be applied unevenly or on an ad-hoc basis by different state authorities. China's proposed procedures are quite different from those of the EU, where data exports are allowed if they are to a country with a positive adequacy assessment, where an exception applies (eg there is data subject consent), or where companies have EU-approved contractual clauses with data recipients. National data protection authorities (and not other regulators) are rarely involved in decisions about specific data exports, except when complaints arise.

### *Notice and consent necessary prior for overseas transfers*

Finally, Article 4 of the Draft Security Measures reiterates the need to adequately inform and obtain the consent of the data subject regarding the 'purpose, scope and type' of any overseas transfer, and the country or region where that recipient is located. The first

(April) draft also required that the data subject be informed of the content or the transfer and the identity of the recipient. The notice obligations have therefore been reduced substantially.

The draft fails to clarify whether such consent may be given at the time of collection (its most likely reading) or prior to the data transfer. Providing notice of the destination of a data export is a form of transparency which is absent from the laws of many countries.

Consent from the data subject will be deemed to have been obtained where it results from the 'active behaviour' of the data subject, such as international phone calls or instant messaging, or cross-border Internet trading. Consent is not required in 'urgent circumstances under which the security of citizens' lives or properties are endangered'.

## Other Recent Regulations

The Draft Security Measures should also be viewed in tandem with the recently promulgated *Interim Security Review Measures for Network Products and Services*, which requires a security review of certain imported foreign IT equipment and services to ensure they are 'secure and controllable.' Under this separate measure, inbound IT equipment and services are to be assessed for various risks, among which is the risk the products or servers will be illegally controlled, interfered with, or interrupted or that the provider of the product or service may use it to illegally collect, store, process or use its users' personal information.

Viewed together, it would appear that China is establishing technology and data security reviews on both the inbound and outbound side, raising concerns this will provide wider latitude for government agencies – including those with links to the country's military and security agencies – to request data and confidential information from foreign companies, particularly those in the IT sector.[11]

## Conclusions: What do China's data export restrictions add up to?

Although it appeared that the Cybersecurity Law, when it was enacted 'does not provide any general rules about data exports,'[12] this can no longer be said, in light of the Draft Security Measures. The rules of general application can now be summarised as:

- Only KIIOs are subject to explicit data localisation requirements through the Cybersecurity Law. These KIIOs must store all data involving "personal information" or "important data" generated from their China operations on PRC servers. Under the April draft of the Draft Security Measures, this data localization requirement would also have applied to all network operators (Art. 2), but this is no longer so under the revised May draft.
- If the conditions in Art. 9 of the Draft Security Measures apply, personal information may not be transferred out of China by network operators, so no data exports are possible and there is in effect implied data localization. In all other situations, personal data exports may be permitted for network operators following the security assessment.
- All data exports involving personal data or important data collected or generated by a network operator within China require a security assessment (Art. 2). This is

[11] Paul Mozur 'China's Cybersecurity Efforts Could Pose New Challenge for Foreign Firms', *New York Times*, 27 December 2016 <https://www.nytimes.com/2016/12/27/business/china-technology-security-review.html?_r=1>.

[12] Greenleaf and Livingston 'China's Cybersecurity Law', p. 5.

normally a self-assessment (Art. 6), but will be done by the relevant sectoral administrator if any of the conditions in Art. 7 apply.
- Network operators must renew the security assessment of its data exports when there is a significant change, or a data security breach (Art. 6).
- Any security assessment must evaluate the matters listed in Art. 8.

When the PRC *Cybersecurity Law* was passed, its data security provisions were criticized by the American Chamber of Commerce in China for being 'vague, ambiguous, and subject to broad interpretation by regulatory authorities.' These concerns were aggravated by the April draft of the Draft Security Measures, as it appeared that they would apply to an even wider range of companies and circumstances, but this is now uncertain.

On the other hand, it can be argued that, if China is to have a data privacy law of international standard, that requires a rule concerning personal data exports which is applicable in all situations. When these measures are finalised, China will have such a rule, like the EU and most other countries with data privacy laws. Whether they will be good general rules is another question. Viewed from a high level, what China is doing is comparable to what the EU has done since 1995 in the limited sense that it is asserting that the free flow of personal data is subordinate to national interests as the EU or China chooses to define them. It would be inaccurate to refer to 'adequacy with Chinese characteristics', but it helps to put these Chinese developments in perspective.

*Scott Livingston is a Senior Associate at Simone IP Services (SIPS), Hong Kong. Graham Greenleaf is Professor of Law & Information Systems, UNSW Australia, and PL&B's Asia-Pacific Editor. Emails: livingston.scottd@gmail.com graham@austlii.edu.au*