China's Completed Personal Information Protection Law: Rights Plus Cyber-security

Graham Greenleaf

[2021] *UNSWLRS* 91
(2021) 172 *Privacy Laws & Business International Report* 20-23

UNSW Law
UNSW Sydney NSW 2052 Australia

China's completed *Personal Information Protection Law*: Rights plus cyber-security

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

(2021) 172 *Privacy Laws & Business International Report* 20-23

On 20 August 2021 the Standing Committee of China's National People's Congress (SC-NPC, not the NPC itself) enacted the *Personal Information Protection Law* (PIPL), the culmination of over a decade of incremental legislative reform.[1] Businesses must adjust rapidly to the law's starting date of 1 November 2021.

Since the first draft of the PIPL was released by the SC-NPC in October 2020, it has been revised in a succession of drafts. One purpose of this article is to detail these changes. The other purpose is to place the PIPL in the context of China's near-complete cyber-security laws, of which it is part.

Final amendments to the PIPL

The first draft of the PIPL was analysed in PL&B in December 2020,[2] as were the subsequent drafts.[3] Of the 74 sections in the final Law, half have had non-trivial amendments since the first draft. Some of the amendments are significant, although none involve fundamental changes to the direction of the first draft.

The **purpose** of the legislation is no longer stated to be to 'ensure the orderly and free flow' of personal information, but rather 'to protect rights and interests in personal information… and to promote the reasonable use of personal information'. It now says it 'is drafted on the basis of the Constitution' (art. 1), although Chinese citizens cannot sue to enforce constitutional rights directly.[4]

Lawful processing changes

The **lawful grounds for processing** (called 'handling' throughout the PIPL) have been somewhat expanded to include 'carrying out human resource management' and 'reasonable scope of handling personal information that has been disclosed by the individual or otherwise already legally disclosed'. It is made clear that consent is not an additional requirement for legitimate grounds of processing (art. 13). Unlike the GDPR, there is no equivalent to protecting the legitimate interests of the controller or a third party. However, administrative regulations may add 'other situations' as lawful grounds (art. 13(7)).

Rights and obligations changes

Controls over **automated decision-making** (art. 24) were already strict, requiring that handlers 'ensure the transparency of the decision-making and that the results are fair and equitable.' Now they are made even tighter, with rights to refuse such decision making, requirements to

[1] For origins and history, see G. Greenleaf *Asian Data Privacy Laws* (OUP 2014), pgs. 204-20.
[2] G. Greenleaf 'China issues a comprehensive draft data privacy law' (2020) 168 *Privacy Laws & Business International Report*, 1, 6-10. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3795001
[3] G. Greenleaf 'Asia's Privacy Reform Bills: Variable Speeds' (2021) 171 *Privacy Laws & Business International Report* 26-29. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899557
[4] Greenleaf *Asian Data Privacy Laws* pgs. 196-7.

provide options 'that do not target specific personal characteristics', bans on 'unreasonable differential treatment of individuals in transaction conditions such as price,' and rights to explanations of such processing. These provisions are at least as strong as those in the GDPR

A right of **data portability** has been added to the right of access (art. 45).

Rights concerning **the deceased** have been added (art. 49), to be exercised by their 'close relatives' 'in order to protect their own lawful and legitimate interests; except as otherwise arranged by the deceased during their lifetime'.

Individuals now have an explicit **right to sue** in the courts a personal information handler that refuses to allow them to exercise their rights (art. 50).

The application of the law to **'state organs'** has been weakened slightly, with consent requirements being replaced by notifications (art. 35). Some exceptions in favour of state organs will also apply to some private sector bodies with 'public affairs management duties' (art. 37). Nevertheless, it remains one of the most remarkable aspects of PIPL that it applies in such a sweeping fashion to state organs – at least on paper.

Administration and enforcement changes

It is now explicit that actions for **compensation** are only available if a breach 'causes harm', and the handlers 'cannot prove that they are not at fault' (art. 69). It is not possible to seek compensation merely because of the breach.

Where large numbers of persons are affected 'legally designated consumer protection organisations' (China's NOYBs) can act on their behalf (art. 70). Litigation by '**privacy NGOs**' has been one of the main driving forces in the first three years of the GDPR.

New penalties for breaches include banning individuals from supervisory roles.

The dominant role of the 'state internet information department' (**Cyberspace Administration of China** (CAC)) is further strengthened, at the expense of departments of the State Council, with a list of new roles added, including drafting 'specialized rules' in relation to small businesses, sensitive personal information and artificial intelligence.

'Platform services' obligations

Special obligations on providers of **platform services** were added by the second draft of PIPL. 'Personal information handlers that provide important internet platform services, have a huge number of users or a complex operational model' (none of which are defined) have additional obligations, the second of which is new in the final law:

1. Establish an independent body comprised mainly of external personnel to conduct oversight of personal information handling activities.
2. Draft fair platform rules, clarifying norms for the handling of personal information by providers of products and services on the platform.[5]
3. Stop providing services to products or service providers on the platform that handle personal information in serious violation of laws and administrative regulations.

[5] Wording in PIPL: ''Comply with the principles of openness, fairness, and equity to draft platform rules, clarifying norms for the handling of personal information in for (sic) the providers of products and services on the platform, and for their obligations to protect personal information'.

4. Periodically publish 'public social responsibility reports on the protection of personal information, and accept societal oversight.'

Obligations 2 and 3 mean that platform operators must therefore discipline their users in relation to privacy. These obligations are imposed on both Chinese and foreign platform operators. Which operators will required to comply is unknown, but initially they are likely to be only the largest.

Extra-territorial application

The PPIL has **extra-territorial application** to processing outside the PRC, including processing for the purpose of providing products and services (marketing) to persons in the PRC, or analysing and assessing the conduct of such persons (like the GDPR), but unlike the GDPR 'other situations provided for by law or administrative regulations' yet to be defined (art. 3). Extra-territoriality under China's law can therefore by expanded by other laws or regulations.

Such extra-territorial processors must designate **representatives within the PRC** and advise their identity to the relevant supervisory authorities (art. 53). Since such foreign processors are subject to all the requirements of this PRC law, this will be a significant risk factor for both them and their local representative. Will foreign processors do so, or will they ignore this requirement? Will organisations already present in China, but doing processing within article 3 overseas, have any realistic choice? Similar representation requirements apply to any party handling personal information at a volume specified by the CAC (art. 52), probably including platform operators.

Data localisation and data exports

The PPIL's provisions on data localization and exports (articles 38-43) have changed through the various drafts, and need to be considered as a whole.

(1) A **copy must be stored** within PRC territory of personal information held by Critical Information Infrastructure Operators (CIIOs) or collected or generated within the PRC and processed 'at the volume provided for' by the state internet information departments (ie the Cyberspace Administration of China (CAC)) (art. 40).

(2) Personal information can only be **exported** 'overseas'[6] when at least one of **four conditions** is satisfied (art. 38):

   a) 'Passing a safety assessment organized by the national network information department' (CAC), unless exempt (under art. 40) from such an assessment by laws, regulations or provisions of the CAC.

   b) 'Having a professional body conduct personal information protection certification in accordance with provisions of the State Internet Information Departments' (led by the CAC). A certification system will need to be established for this purpose, with clarification of whether certification is per transfer, per transfer type, or per business, and for what duration.[7]

[6] The first draft PIPL said 'outside the PRC', so it is possible but uncertain that this prohibition might also include Hong Kong.
[7] See DLA Piper 'China: New draft national, harmonised data protection law for Mainland China' *Lexology*, 26 October 2020.

c) 'Contracts concluded with the overseas recipient parties in accordance with standard contract drafted by the [CAC] [which] agree upon the rights and obligations of both parties.'[8] It seems these will play an equivalent role to the GDPR's Standard Contractual Clauses (SCCs).

d) 'Other conditions provided for by laws, administrative regulations, or provisions of the State Internet Information departments'.

In addition (and not as alternative grounds for export), three other conditions must be satisfied: (i) the export must be necessary ('truly need') 'due to business requirements' (art. 38); (ii) the consent of the individuals affected must be obtained, after provision of data about the overseas transfer (art. 39); and (iii) a 'personal information protection impact assessment' must be conducted (art. 55), with specific requirements, and a copy retained (art. 56). The cumulative effect of these requirements may be prohibitive.

Another amended provision concerning conditional exports is that 'requests for the provision of domestically-stored personal information from foreign justice or law enforcement' authorities, information handlers (controllers) must not provide this information 'without the permission of the competent organs of the PRC' (art. 41).[9]

(3) If any of the above conditions for exports (a) – (c) are implemented in very restrictive manner by CAC, export would in effect be **prohibited**). Two clauses create new and uncertain types of prohibitions, by allowing retaliatory measures to be taken by China against overseas companies, countries or regions (arts. 42 and 43).[10] They create a new type of risk for companies, that their own governments take actions that could result in their country becoming subject to Chinese retaliatory actions which could adversely affect their company.

An alternative basis for exports is that 'international treaties and agreements' which 'have requirements for the provision of personal information overseas and so forth' 'may be implemented' (art. 38).

Adequacy or negotiation?

Are these export conditions 'just Chinese adequacy'? None of the conditions in article 38(2)(a)-(d) refer directly to the state of the law in the receiving country, so conditional exports in China have little similarity to 'adequacy' in the EU. Also, there are no objective criteria for consent to export, no role for an independent Data Protection Authority (the PIPL does not provide for one), and no provisions for data controllers to appeal to a court against a CAC decision. CAC control over the above conditions (a)-(d) amounts to CAC discretion to prohibit some categories of export completely. Some commentators conclude that this is likely to result in *de facto* export prohibition because 'companies will greatly reduce cross-border transfers of

[8] The first draft referred to a contract with the overseas recipient where the rights and obligation, and oversight, comply with 'standards provided for in this Law'. The 2nd and 3rd drafts of the law tightened this condition very considerably. The 2nd draft appeared to say that standard clauses developed by the CAC would play an equivalent role to the GDPR's Standard Contractual Clauses (SCCs), and would probably be compulsory. The 3rd draft went further, with some commentators interpreting it as requiring that the contract be tripartite, with the CAC also as a party (see Galaad Delval 'China: The draft PIPL – Shifting into third gear' *Data Guidance*, June 2021) This interpolation of the CAC into the contract formation process may have had a 'chilling effect' on the enthusiasm of companies to use this option, but it does not appear in the final version enacted.

[9] The first draft provided that where it is necessary for 'international judicial assistance or administrative law enforcement assistance', approval by the relevant regulatory authority is required, unless a treaty or agreement concluded by or participated in by the PRC provides authority. The enacted version of art. 41 is very different.

[10] For details, see Greenleaf 'China issues a comprehensive draft data privacy law'.

personal information, as all available transfer mechanisms now require heavy administrative undertakings'.[11] An unfettered government discretion to prohibit export of unspecified categories of personal data, such as the CAC can be argued to have, is one of the types of data localisation about which its opponents (including advocates of the 'free flow of personal data' that accept conditional restrictions) have the highest concerns.

Rather than setting out clear and objective conditions for the export of personal data, PIPL's approach is to turn this into a negotiation with the CAC or other PRC authorities. This is consistent with the **international engagement** requirement that 'the state is to actively participate in the formulation of international rules for protecting personal information, and promote mutual recognition of rules and standards for the protection of personal information with other countries, regions, and international organizations' (art. 12). When coupled with the allowance of data export provisions in treaties and agreements (art. 38, above), this seems to open the way for China to negotiate mutual data export agreements, multilateral or bilateral. It remains to be seen whether this approach will play a significant role in China's international engagements such as its application to become a party to the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), or in relation to the 165 countries that it has agreements with under its 'Belt and Road Initiative'.[12]

PIPL's context: China's cybersecurity laws

From its role in regulating data exports, it is clear that PIPL also plays a role in China's emerging cyber-security structure. The *Cybersecurity Law* (CSL)[13] of 2016 and the *Data Security Law* (DSL)[14] of 2021 also refer to more strict data localization and export rules that are to be developed to apply to 'critical information infrastructure operators' (CIIOs), and to other data handlers of 'important' data, but both CII and 'important data' remained without definition[15] until the new *Regulations on Critical Information Infrastructure (CII) Security Protection* ('CII Regs*)*, which took effect on 1 September 2021.[16]

The CII Regs set out general factors relevant to a classification of CII (mainly concerning the extent of harm likely to flow from its disruption), and delegates responsibility for identifying CII and determining CIIO status to 'individual sectoral regulators and responsible government departments, acting under supervision of the [CAC]'.[17] However, the effect of a classification as CII on the export of personal data remains unclear.[18] PIPL requires that a copy be held within

[11] Galaad Delval op cit.
[12] H. Davidson 'China owed $385bn – including 'hidden debt' from poorer nations, says report' *The Guardian* 1 October 2021 <https://www.theguardian.com/world/2021/sep/30/42-nations-owe-china-hidden-debts-exceeding-10-of-gdp-says-report?CMP=Share_iOSApp_Other>
[13] G. Greenleaf, and S. Livingston 'China's New Cybersecurity Law – Also a Data Privacy Law? (2016) 144 *Privacy Laws & Business International Report* 1-7.
[14] J. Li and J. P. Tomaszewski 'China's New Data Security Law' *Lexology* 9 July 2021; a translation of the Data Security Law is available from China Law Translate.
[15] The DSL says that both it and the CSL require that 'security management measures for the export' of both data collected or produced by CIIOs, and 'other important data' are to be drafted by the CAC in cooperation with the 'relevant departments of the State Council' (art. 31).
[16] For a concise analysis of the relationship between the CII Regs and the PIPL, see Freshfield Bruckhaus Deringer authors 'China's restrictions on cross-border data transfer' *Lexology* 15 September 2021.
[17] ibid
[18] The Regulation has been described as 'bizzarely' totally silent on the question of what implications a classification of 'critical information infrastructure' will have for the export of personal data: Bird & Bird LLP 'China Released Regulation on Critical Information Infrastructure' *Lexology*, 8 September 2021.

the PRC, and that a safety assessment organized by the CAC is required, unless there is an exemption (art. 40).

'Important data', which could include some personal data, is also to have special export rules formulated by the CAC (CSL art. 37). The CSL and DSL do not define 'important data', but the DSL delegates to regional and sectoral regulators to formulate catalogues of important data, and to designate some of it as 'core state data' (art. 21).

Conclusions: Protecting rights and cyber-security interests

The result of the amendments in the final version of the PIPL is that the law is now less ambiguous, and overall it gives stronger protection to data subjects. Almost all of the changes detailed above benefit data subjects. Some do not benefit data controllers outside the PRC. The result is a modern and sophisticated data privacy law, influenced by many advanced aspects of the GDPR, and which in a few respects may be stronger than the GDPR. Of course, any such judgments must await the law's operation in practice, but with a starting date almost immediately, evidence may be available soon. It must also be assessed in light of the PRC's state surveillance practices.

More than most data privacy laws, this law also has to be considered as part of China's cyber-security protections, because there are many ways in which the data export, data localisation, extra-territorial, retaliatory and 'platform' provisions can be utilised to further the PRC's foreign policy objectives.

China's law is both sufficiently in the mainstream of GDPR-influenced laws, and sufficiently distinctive that it could become the first significant competitor to the EU in obtaining influence over development of other national data privacy laws. It is possible that alternative models will emerge when India finally enacts its law, or when the US discovers that it needs to compete for global influence with its own modern data privacy law, abandoning the pretence that 'notice and consent' is sufficient.