HINSHAW

China's New Privacy Law: Both a Shield And a Sword

Hinshaw Alert | 4 min read
Sep 17, 2021

On August 20, 2021, the People's Republic of China (PRC) passed a sweeping data protection law, the Personal Information Protection Law (PIPL), set to take effect on November 1, 2021. Although the PIPL appears to borrow heavily from the European Union's (EU) General Data Protection Regulation (GDPR), it is unlikely to be similarly interpreted and enforced. Indeed, unlike the EU, the PRC is a communist country that has moved between various degrees of authoritarianism throughout its history. The Chinese Communist Party, the sole governing political party of the PRC, is naturally focused on maintaining power. Through that lens, the PIPL can be viewed as a national security measure that advances the geopolitical and economic interests of the PRC, with data privacy and protection being a useful and populace pleasing component.

Support for that conclusion can be found within the first twelve articles of the PIPL. For example:

- Article 2 - The personal information of any natural person shall be protected by law, and *no organization or individual may infringe* upon the personal information rights and interests of any natural person.
- Article 10 - *No organization or individual may illegally collect, use, process, or transmit other people's personal information*, or illegally trade, provide, or disclose other people's personal information, or engage in the processing of personal information *that endangers the national security or public interests*.
- Article 11 - *The State establishes a sound personal information protection system, prevent and punish the infringement of personal information rights and interests, strengthen the publicity and education on personal information protection, and promote the formation of a good environment for the government*, enterprises, relevant social organizations and the public to jointly participate in personal information protection.

As the italicized language suggests, the obligations of private actors are different from those of the State, or interchangeably, the government. Private actors are explicitly prohibited from infringing on personal information rights or from illegally using personal information, but not the State. In fact, Article 11 makes clear that this regulatory environment was created, in part, for the benefit of the government. Chapter 2, Section 3 of the PIPL highlights this point by providing the State with a possibly important exception to compliance, *i.e.*, the law is not applicable to the State where it is "…performing its statutory duties…under the procedures prescribed by laws and administrative regulations…" Given the context under which this provision must be analyzed, this could be

read quite broadly and, ultimately, act as a shield if the government is accused of violating the strict privacy rights set forth in the PIPL.

Of course, this also begs the question, what is a good environment for the government? Starting from the premise that knowledge is power, having near unfettered access to the personal information of a fifth of the world's population means that threats to governmental power can be quickly contained and extinguished. As we have seen, civil disobedience, for the most part, now starts online. If the government is tuned in and can get ahead of expressions of discontent, then it can better protect its interests. Moreover, a government that can regulate, demand data from and punish tech platforms that collect, process and disseminate information harmful to its interest can also easily identify the source of a threat and disable it.

However, threats come not only from within, but also from outside the state. To that end, the PIPL provides the following:

- Article 42 - For any overseas organization or individual whose personal information processing activities damage the personal information rights and interests of citizens of the People's Republic of China, or endanger the national security or public interests of the People's Republic of China, the State cyberspace administration may include such overseas organization or individual in the list of restricted or prohibited provision of personal information, announce the same, and take measures such as restricting or prohibiting provision of personal information to such overseas organization or individual.
- Article 43 - Where any country or region takes discriminatory prohibitive, restrictive or other similar measures against the People's Republic of China in respect of the protection of personal information, the People's Republic of China may, as the case may be, take reciprocal measures against such country or region.

In short, foreign companies can be blacklisted from transferring information out of the PRC if their processing is perceived as a threat to national security or the public interest and other countries can expect reciprocal treatment in connection with their approach to cross-border data transfers. In other words, the PIPL contains not only a shield for governmental intrusions, but also a sword. Presumably, the threat of reciprocal treatment is directed to the EU, which prohibits the transfer of personal data to countries without adequate levels of protection in place. Essentially, this could be interpreted as: "if you find us inadequate, we will find you inadequate."

Being able to control the flow of such massive amounts of data puts the PRC in a unique position on the world stage and is akin to it controlling a major asset or a natural resource like oil or cobalt. Data powers the algorithms that powers artificial intelligence, which many believe will be a key part of the "Fourth Industrial Revolution." The PRC has made no secret of its plan to not only lead in this field, but to dominate it. As such, the PIPL may be yet another step toward achieving that dominance while simultaneously appeasing rising concerns about privacy stemming from the PRC's social credit system and the unscrupulous acts of private actors within the State. However you view it, practitioners and businesses should not yet assume that the PIPL will be another GDPR, which is the product of an altogether different legal system.

Related People

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity