MAYER | BROWN

Podcast

Tech Talks

Unpacking the China Data Laws

August 28, 2023

Announcer
Welcome to Mayer Brown's Tech Talks Podcast. Each podcast is designed to provide insights on legal issues relating to Technology & IP Transactions, and keep you up to date on the latest trends in growth & innovation, digital transformation, IP & data monetization and operational improvement by drawing on the perspectives of practitioners who have executed technology and IP transactions around the world. You can subscribe to the show on all major podcasting platforms. We hope you enjoy the program.

Julian Dibbell
Hello and welcome to Tech Talks. Our topic today is "Unpacking the China Data Laws." I'm your host, Julian Dibbell. I am a senior associate in Mayer Brown's Technology & IP Transactions practice. I'm joined today by Gabriela Kennedy. Gabriela is a partner in our Hong Kong office and head of the Asia IP and TMT group. She is also co-leader of Mayer Brown's global Intellectual Property practice and a member of the firm's global Cybersecurity & Data Privacy and Technology & IP Transactions practices.

Gabriela, welcome back. I know you were on of the podcast just about two years ago to talk to us about China's data laws and their potentially global impact. At the time, the first of those laws, the so-called cybersecurity law, had been in effect for four years, and it was just being joined by the data security law (the DSL) and the Personal Information Protection Law (PIPL), both of which took effect in late 2021. These were all relatively new laws at the time. I'm hoping that today you can give us a more informed update, now that the world has had a couple of years to live with these laws and see how their effects are playing out and how they're interacting with each other. I guess we should probably start with a brief refresher on the basics, if you could help us out with that.

What are these laws and what do they each cover?

Gabriela Kennedy
Thank you, Julian, and thank you for inviting me back to be a guest on your podcast. These laws are very, very interesting.

CSL, as you noted, came into effect in June 2017, and together with the DSL, the data security law, form a framework around the security of data that is collected in China. So in very simple terms, it is all the business data that is being collected by a company during the course of doing business. And you might ask, well, I've had the CSL. It came in in June 2017, why would I need a data security law? What is that adding to what I already have on the books? CSL was focusing mostly on electronic data while DSL does a sweep-all and catches analog data as well. The personal information protection law that came, the PIPL

that came in November, focuses largely and entirely on personal information. Interestingly enough, CSL, prior to PIPL, had some provisions that dealt with personal information.

So the question now is, what do you do with those provisions that existed under CSL? Are they swept under the carpet? Am I just looking now at what is happening under PIPL? That imposes obligations that are known for anybody who does data privacy or has had to worry about data privacy for their companies relating to data controllers.

Though interestingly enough, the terminology in China is slightly different. A data controller, confusingly, is called a personal information processor, but for the purposes of this talk, I'm going to refer to them as data controllers because that is a term that is more known to our listeners.

Though they have different purposes, these three pieces of legislation… the first two, as I said, provide a high-level framework that relates to the security of data, cyber security and security of data, and they impose certain restrictions on what can be done with that data: whether or not it has to be localized, and if there are possibilities to transfer that data across borders, what would be the conditions for that to happen? And PIPL really gives a comprehensive framework for the protection of personal information with some known elements that really relate to international concepts. But there will be very Chinese characteristics applied to them, so I hope this answers your question.

Julian Dibbell
Sure. Then there are three separate laws, but there's clearly some overlap among them. Is that correct?

Gabriela Kennedy
There is overlap. As I said, the CSL and DSL relate to the security of data and they relate to personal and non-personal data. They have some overlap in terms of some of the concepts that I used. You will, when you read these laws, come across terms such as important data, core national data. Those terms keep appearing in DSL and CSL, but they are different and there are different explanations for them. These terms are deliberately vague because they can be very malleable, and in fact it was only towards the end of last year that we had some clarifiying guidelines vis-a-vis how the officials are going to interpret the definition of core national data versus important data. There are certain commonalities in terms of requirements—the intel of what companies need to do to prepare and to ensure that they have a stable framework that would not damage and affect national security. That relates to a multi-level protection scheme. So every company has to determine where they are in terms of their level of security risk should an incident occur, and that is something that appears under both DSL and CSL.

We also have certain commonalities, as I said, in terms of purpose and scope—so, three areas: purpose and scope, some definitions and concepts, and some requirements that carry through some of these legislations. So the point that I would like to make here is, you cannot look at these laws in isolation. If you're a company that tries to comply with data laws in China, do not focus just on PIPL, right? What has happened since PIPL came into force was especially for foreign companies that had already a heightened understanding of data privacy regulations internationally. They zoomed in and tried to focus on compliance with PIPL, forgetting about compliance with DSL and CSL.

And these legislations are intertwined. You cannot look at them in isolation, and you must remember that the regulator under these three pieces of legislation is the same. So should any investigation occur or a breach under one of the laws, then the investigation can extend to compliance under the other laws.

Julian Dibbell
Alright, well, there's three laws; they interrelate. Tthere's a certain amount of complexity there, but there are laws. They're written down. We saw the letter of the law. Even, you know, two years ago when you were with us last. But what we're hearing is, nonetheless, you can go read the laws and in theory know how to comply with them. It's actually turning out to be fairly difficult in practice, to comply with these laws; why is that?

Gabriela Kennedy
Many, many reasons. The first is the fact that the laws, as I said, are very vague and broad. So you're expecting to have some guidelines and clarification to know exactly how compliance is going to take place because there are fine details on what filing requirements you have—and there are many. There have been piecemeal guidelines and regulations and what made compliance very difficult was the fact that these were issued, let's say, draft measures or draft guidelines and they stayed in draft for months and months and months, sometimes 10 months, 11 months, before they were finalized, which left a big question mark. The companies think, how am I going to comply in the meantime? I know I have the vague idea of what I need to comply with, but I don't know the specifics and what exactly I need to do. So the advice and the wisdom had been up to the point where an actual guideline gets finalized to try and comply by looking at the draft as much as you can.

I also mentioned earlier that there are very vague definitions, so it's difficult to know. Am I going to be categorized as a critical information infrastructure under CSL? And when I say critical information infrastructure, normally people think of electricity grid, telecommunication company, big infrastructure companies. Am I going to be a network operator, which is everybody else? Everybody else is connected to the network. Am I collecting data that is important data? Well, I don't know, because that definition and the way a regulator will look at it will depend on an economic context, geopolitical context, the weight of my business in that country; it can change. As I said, we've just had some measures that clarify, to a certain extent, only in December last year.

The most, most, most difficult point and bit for most companies has been the multi-level protection scheme because that requires a lot of work. You need to do self-assessments, you need to do third-party assessment. You need to file gradings with the Public Security Bureau, which is like the police. You need to have network governance. And you need to submit an evaluation report and you're not quite sure whether you're on Level 1 or Level 2. Level 1 and Level 2 are the lowest levels, and the higher up you go towards Levels 3, 4, and 5, the more obligations you have, so there's a lot of uncertainty as to where you are categorized. I guess most companies would want to be on Level 1, but in reality most of them end up on Level 2. And then you're having to determine what you have to do in that sense. There was a lot of uncertainty about transfer of data, so probably headlines said, China is imposing data localization, yes and no.

So transfers are possible, but you have to go through a lot of hurdles, right? There are certain scenarios that permit you to transfer. You know the data and you know the one that, again, most companies focus on the data privacy laws, is PIPL. There are three ways in each in which you can transfer data across borders. There's a security assessment, and there's a obtaining a certification which is conducted by an accredited body, or, the one that everybody's been waiting for, executing a standard contract, because that is something that we understand we've seen in other countries. We can transfer, we can say, "Well, I'm used to that. I've done it. It's probably not as painful of a process." Well, yes and no.

Julian Dibbell
But they are similar to the standard contractual clauses that we see in EU-US Data transfers.

Gabriela Kennedy
Similar in name, dissimilar in every other respect because you have to go through a number of processes and things that you have to do. You have to do a privacy impact assessment. You have filing requirements that are quite onerous. There's a whole list of things that you have to file, and there's a deadline. The standard contract has just been finalized in March. The actual filing requirements were issued in June this year, and there's a deadline to file your standard contract by the end of November, by the 1st of December. So there's a flurry of activity at the moment for most companies to finalize their standard contracts. But there are still uncertainties that remain even with a clarification that was issued in June this year.

Julian Dibbell
So you mentioned a few times, assessments, you mentioned certifications, there were potential approvals. How many of these are there, packed up in these various laws in order for companies operating in China to be fully compliant?

Gabriela Kennedy
Oh my goodness. So let me just very, very briefly (and I hope I don't scare the audience or the listeners too much) take you through some of them. Not an exhaustive list, but just some to give you a taste of what you have to do to comply.

So under CSL, you have to satisfy the MLPS, right? That involves a self-assessment. If you're a network classified as level 2, it's a CII operators' assessment. If you are a CII, you have filing requirements, you have a security assessment, as I said, that you have to do; you have an official security assessment that you have to file. Under DSL, if you are handling core national data or important data, you have to have a risk assessment just for that; you have to have a security assessment. In the unfortunate event that you have an incident, you have to go through a data security incident. If you want to get data transferred out of China, you need prior approval from a relevant PRC authority. So DSL has extraterritorial jurisdiction, as has PIPL, which is very, very interesting. CSL doesn't, but DSL does, and in essence it stops a company from transferring data, let's say under compulsion of a court order in the US. That cannot happen unless you have gone through these processes and you have obtained the prior approval of the PRC regulator. So if you have a deadline imposed to you, say, by a US Court in a discovery process, that is going to cause a bit of a headache. And under PIPL, you have security assessments, you know, especially for cross-border data transfers, previously impact assessments, and those are relevant when you're doing transfers, but also if you're handling sensitive information.

It is quite a lot of assessment. I would say some assessments you can do yourselves, and others may have to be done by third parties and the third parties, depending on where you are on the MTLS level, might be particular authorized third-party institutions. There's a list and you've got to use them.

Julian Dibbell
OK, that's a lot. But my understanding is, generally, these apply to companies operating in China. Is that right?

Gabriela Kennedy
It applies to any company that's suddenly CSL, any company that operates in China and is connected to the network, right? So it applies. You are on the grid. There is an ethos of, if there is an incident or cyber incident, this obviously will affect your operations but will the effect be wider? And that's why the concern over it. DSL, as I said, is about the security of data. It's more protectionist about the data that is being gathered in China and it may be or may not be in response to provisions in foreign acts that prevent that, that relate to access to data that is available in China. OK, so ring fencing data within national borders, that's the ethos.

PIPL has extraterritorial effect in the sense that, if I'm collecting information about individuals who are located in China—so I have a website and I'm selling, I'm offering services and products even though I don't have a presence in China, but my website is accessible in China and I'm not restricting access. I am not discouraging and conducting business with people who are and offering services to people who are in China, then I'm going be caught by PIPL. Or if I analyze and evaluate the activities of individuals located in China, then I am going to be caught by that and there will be a requirement to appoint to establish a dedicated entity or a pointer representative within the PRC that is responsible for matters relating to personal data handling in China that I am conducting. So you need to report to the authorities who that entity is. That will be your designated entity for the purposes of PIPL.

Julian Dibbell
And that's for any person doing business with China and potentially handling the personal data.

Gabriela Kennedy
Correct.

Julian Dibbell
So what are then some of the key challenges companies face in in trying to be compliant with these laws?

Gabriela Kennedy
There are many. As I was saying earlier, there are privacy impact assessments required, but to be conducted under various circumstances under PIPL. Who's going to conduct that? You know, how are you going to do it? PIPL also you have separate consent requirements for certain types of personal data. There are also uncertainties in application. There are nebulous concepts. As I was saying, important data, core national security data and what certainty I may have today about whether or not I can collect important data, may change tomorrow depending on the geopolitical context, depending on many, many things, and depending on new classifications that might happen. The cross-border transfer restrictions are very onerous. So on the whole, compliance has been quite a headache for many companies and many have adopted a wait-and-see attitude and have looked at what is the general shared wisdom amongst peers in terms of their road to compliance.

Julian Dibbell
So I imagine another layer of risk here is in companies who do business with China, they have third parties that they rely on as well, for many of their services or products. What provisions should companies doing business in China, or with China, include in their contracts with these third parties, especially given the extraterritorial application of these laws?

Gabriela Kennedy
Again, it depends on the sector, depends on what you're doing, but you want to have representations and warranties that say that your Chinese partner does not deal in important data, so you don't want to be caught out inadvertently. Have they obtained all necessary consents? Have they conducted the necessary impact assessment? They need to give you a sort of a general warranty that they're in compliance. If we're talking about supply chain and if they have a third-party access, there are quite strict obligations in terms of reporting an incident. Sometimes it's a matter of a couple of hours, right? It's eight hours under DSL. If you are transferring data, remember that if you're transferring data to a business partner in China, the data that you have transferred becomes, all of a sudden, subject to the data laws in China. So that's something that you need to be aware of and think of how you are going to frame that contractually to get protection.

Many companies will require a standard contract now. If you're doing business with a Chinese company and they will be transferring some data to you and you're located overseas, they will ask you to sign a standard contract.

Julian Dibbell
This is the standard contract we were talking about earlier, right?

Gabriela Kennedy
Yes, and they are unlike what we are used to in other jurisdictions. This is something that is non-negotiable. It's been given. It's been provided and it's in a form that cannot be changed. So you have to sign the standard contract or otherwise go through the other two mechanisms for data transfer, which involve a lot of assessment certifications that nobody wants to do.

Julian Dibbell
OK, so consequences of not complying. What are we seeing so far in terms of enforcement of these laws? What are the risks there?

Gabriela Kennedy
Well, let's just look at what the statute says. Basically fines under CSL, revocation/suspension of business license under DSL, and PIPL has fines that are tied to global turnover. So 5% of your turnover in China or quite a high fine of $100 million. The first couple of years under CSL, we saw a lot of enforcement focused on technology companies in China and the fines were not that particularly high. The one enforcement that you know caught everybody's attention was the enforcements against DD, which was fined $1.2 billion US. They had 25 apps that were suspended for the duration of the investigation, and other potential risks of enforcement include being placed on a list in relation to social credit, you know, as a company. What that means is that your ability as a company in China to get a loan might be affected, your ability to compete and try to get government contracts, or getting involved in particular kinds of projects is going to be limited.

The one thing that we have seen recently is a beginning of enforcement against foreign companies that operate in China. That started about a year and a bit ago when we had Walmart subject to a warning because of certain practices of their operations in southern China, and more recently the regulator coming and conducting and beginning investigations and entering offices of foreign consultancies in China.

Julian Dibbell
Ah. Alright, so be on the lookout, foreign companies. Are there other laws? Other regulations on the horizon that companies should be looking out for?

Gabriela Kennedy
Yes. We've just had, last week, draft measures on facial recognition and biometric identification, which are quite interesting, subject for another podcast, perhaps? There's also draft regulation on audit measures in relation to personal data compliance, so an audit depending on where you are and the volume of data that you are handling could be annual. We have had interim measures on Gen AI. Of course, you know, everybody's talking about artificial intelligence and Gen AI, and we've had new anti-espionage laws coming in in July this year, which will join the data laws now because they also look and focus on the transfer of any information related to national security and interest. So it's an add-on to the data security law.

Julian Dibbell
Finally, any other issues and that our listeners should be looking out for?

Gabriela Kennedy
I would say that, if you have China-facing business operations and you haven't yet started to look at these laws, now is the time to do so. And the first step that a company could take is to at least articulate the road map and figure out some of the critical steps that should be taken. MLPS would be one, and secondly would be looking at the our privacy practices and procedures and potentially considering standard contracts.

Julian Dibbell
Thanks very much, Gabriela; very helpful and we appreciate your insights. Thank you for coming on the podcast today. Listeners, if you have any questions about today's episode or an idea for an episode you'd like to hear about, anything related to technology and IP transactions and the law, please email us at techtransactions@mayerbrown.com. Thanks for listening.

Announcer
We hope you enjoyed this program. You can subscribe on all major podcasting platforms. To learn about other Mayer Brown audio programming, visit mayerbrown.com/podcasts. Thanks for listening.