

PANORAMIC NEXT

# Privacy & Cybersecurity

CHINA

LEXOLOGY



# Privacy & Cybersecurity

2024

---

Cybersecurity continues to represent a growing risk for companies around the world, with cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' continuing to grow on a global basis.

---

**Generated: July 23, 2024**

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research



Explore on Lexology [↗](#)

# China

[Jingyuan Shi, Yuchen Lai](#)

[Simmons & Simmons](#)

## Summary

### PROFILES

About the lawyers

### Q&A

What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

### THE INSIDE TRACK

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

How is the privacy landscape changing in your jurisdiction?

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

## Profiles

### ABOUT THE LAWYERS

Jingyuan Shi is the key contact for the Shenzhen office of Simmons & Simmons, and a partner leading the TMT practice in the Greater China region. She is a PRC-qualified lawyer and a practising solicitor in England and Wales. Jingyuan specialises in data and technology laws. She has supported a large number of telecoms, media and technology (TMT) companies, strategic and financial investors in the TMT industry, asset managers, financial institutions, fintech companies and life science companies on an impressive selection of mandates, including data compliance, PE/VC and M&A transactions, regulatory and intellectual property. Jingyuan is regularly invited to speak at industrial events. She is also a regular contributor to the Simmons & Simmons website and WeChat account, and for the China chapters of Lexology Getting The Deal Through: Fintech (2017–2023), Telecoms & Media (2017–2021) and Market Intelligence: Privacy and Cybersecurity (2021–2022).

Yuchen Lai is a legal executive in our Shenzhen office and dual-qualified in the PRC and England and Wales. She works extensively for international and Chinese telecoms, media and technology (TMT) companies, strategic and financial investors, financial institutions, asset managers, fintech companies and life sciences companies. She advises on a wide range of compliance issues such as data and wider regulatory compliance, as well as corporate transactions. Yuchen has a strong focus on China data advice and has in-depth knowledge and rich experience in Chinese and global data compliance projects.

## Q&A

### WHAT WERE THE KEY REGULATORY DEVELOPMENTS IN YOUR JURISDICTION OVER THE PAST YEAR CONCERNING CYBERSECURITY STANDARDS?

Over the past year, we have seen material regulatory updates in relation to cybersecurity matters in China, which, for the purposes of this chapter only, refers to mainland China, without taking into account the laws and practice in Hong Kong SAR, Macau SAR and the Taiwan region. The one with the widest influence is the adjustment of China's regulatory regime of cross-border data transfer (CBDT).

On 22 March 2024, the Cyberspace Administration of China (CAC) issued the Provisions to Promote and Regulate Cross-Border Data Flows (the Provisions), which took effect on the same day and introduced exemptions and relaxations to certain compliance requirements under China's CBDT regime.

Prior to the implementation of the Provisions, a personal information processor (ie, equivalent to a 'data controller' under the EU General Data Protection Regulation (GDPR)) transferring personal information out of China (ie, a data exporter), would have to adopt one of the three transfer mechanisms (Safeguards), depending on the nature of the data exporter and the amount of the data subjects involved:

- passing a security assessment conducted by the CAC (the Security Assessment), which is in essence a process of administrative approval;

- concluding and filing a standard contract formulated by the CAC (the Standard Contract), which shares a fair amount of similarities with the EU's Standard Contractual Clauses for international data transfer (the EU SCCs), whereas maintaining significant unique features; or
- obtaining a certification for personal information protection (the issued by a professional agency designated by the CAC).

With the implementation of the Provisions, activities and data exporters that fall within the exemptions are not required to adopt the Safeguards before transferring personal information out of China.

Previously and since the implementation of three Safeguards in late 2022, cross-border data transfer compliance has been a challenging issue for many businesses in China. The long review process and low pass rate of the Security Assessment and Standard Contract filing have cast a shadow on the operation of many multinational companies. Therefore, the issuance of the Provisions is widely seen as a business-friendly initiative from the Chinese regulators, as it demonstrates the Chinese government's effort to lessen burdens from businesses and reassure foreign investors of the friendly policy environment and steady adherence to the 'opening-up' policy.

The exemptions can be grouped into the following four categories.

- *Small-scale transfer: Preconditions for this exemption include that: (1) the Data Exporter is not a critical information infrastructure operator as identified by the competent regulators; and (2) counting from 1 January of the current year, the Data Exporter has transferred personal information of fewer than 100,000 individuals and no sensitive personal information outside of China (Article 5(4) of the Provisions). This exemption is particularly relevant to unregulated small and medium enterprises as well as larger companies conducting business-to-business activities, where the data transfer usually involves a relatively small number of data subjects.*
- *Specific exempted scenarios: These include:*
  - contract necessity – where the transfer of personal information is truly necessary to perform a contract to which the individual is a party. Typical examples mentioned under the Provisions include cross-border e-commerce, postal and delivery service, payment and remittance, account opening, overseas travel booking, and visa application and examination services (Article 5(1) of the Provisions). This exemption may provide particular relief for organisations that conduct cross-border retail businesses;
  - human resource management – where the transfer of personal information is truly necessary to conduct cross-border human resource management in accordance with employment rules or collective employment agreements established according to law (Article 5(2) of the Provisions); and
  - emergency – where the transfer of personal information is truly necessary under emergency situations for protecting the life, health and property of a natural person (Article 5(3) of the Provisions).
- *Negative lists in free trade zones: The Provisions also grant power to free trade zones (FTZs) to publish their own 'negative lists' (subject to approval by provincial*

cybersecurity authority and filing with the CAC and national data management authority). Where a Data Exporter incorporated within a FTZ transfers personal information not on the FTZ's negative list, the transfer will be exempted from the Safeguards (Article 6 of the Provisions).

- *Personal information 'passing through' China: Preconditions for this exemption include: (1) the personal information concerned that was originally collected or generated outside China; and (2) when processed within China, no personal information of China-based individuals or important data has been attached to the personal information concerned (Article 4 of the Provisions). This exemption may be particularly helpful for those organisations that operate regional headquarters, data centres or offshore data processing services in China.*

In addition to the Provisions, more regulations, standards and draft rules were also published in the past year to supplement China's cybersecurity and data protection regime realised by the Cybersecurity Law, the Personal Information Protection Law (PIPL) and the Data Security Law. To name a few, these include, among others, the draft sectoral data security regulation issued by the People's Bank of China (PBOC), the draft regulation on personal information protection compliance audit, the draft regulation on the deployment of facial recognition technology and the draft regulation on cybersecurity incident reporting.

#### **WHEN DO DATA BREACHES REQUIRE NOTICE TO REGULATORS OR CONSUMERS, AND WHAT ARE THE KEY FACTORS THAT ORGANISATIONS MUST ASSESS WHEN DECIDING WHETHER TO NOTIFY REGULATORS OR CONSUMERS?**

The Cybersecurity Law requires network operators to notify competent regulators of cybersecurity incidents including personal information breaches, but it does not go on to provide details about the key factors to be assessed. A set of existing lower-level regulations and standards provide guidelines in this regard. The reportable incidents usually include cyberattacks, hacking, malware, virus and human or equipment failure that may cause significant damage to society and the general public. Subject to the affected areas and degree of damage, there are different categories of reportable breaches. The key factors or impact of an incident that an organisation must assess include: (1) internet access in geographic areas (eg, single or multiple provinces, or even the entire country); (2) operation of major websites or platforms (eg, e-commerce websites with millions of active users); (3) number of users affected (a minimum of 100,000 users should ring alarm bells); (4) loss, theft or falsification of state secrets, or important or core data that may cause significant damage; and (5) a catch-all scenario applicable to other factors, judged by the discretion of the organisation suffering the breach incident.

In December 2023, the CAC published the draft Administrative Measures on Reporting Cybersecurity Incidents, which are still pending finalisation. This draft categorises cybersecurity incidents into four groups, namely catastrophic incidents, severe incidents, significant incidents and normal incidents. An initial report on the catastrophic or severe incidents must be submitted within one hour, using a template form formulated by the CAC. The draft does not specify the initial reporting timeline for significant and normal incidents. Further, a post-incident report summarising the cause, disposal measures, damage, accountability, remediation and lessons learned shall be submitted within the five days following disposal of the incident.

The PIPL requires the personal information processors (note the definition of personal information processor under Chinese law is essentially equivalent to the concept of a 'data controller' under the GDPR) to notify the competent regulator and relevant individuals once a personal data breach is detected. If the processor can take measures to effectively avoid the damage caused by data breaches, then it may decide not to notify the affected individuals. However, if the data protection regulators find the breaches may cause damage to individuals, they can request the processor to notify the affected individuals regardless. There is so far no general hard time requirement on when this report must be done under the PIPL, but we recommend data processors to report as soon as possible if initial assessments point to a report.

ie, it is worth noting that in addition to the cyber and data regulator (ie, the CAC), various market players may also be required to report cybersecurity and data incidents to their sectoral regulators, and there exist sectoral rules with more specific provisions on this issue. For example, for financial institutions, according to the Implementation Measures for Protecting Financial Consumers' Rights and Interests, which took effect on 1 November 2020, reports to consumers and the financial regulators must be made within 72 hours. The Measure for Supervising the Risks of Information Technology Outsourcing Activities by Banking and Insurance Institutions, which took effect on 30 December 2021, provides that banks shall report to the China Banking and Insurance Regulatory Commission or its local counterparts within 24 hours of any client personal information breach or data damage/loss during IT outsourcing activities. The Measures on Reporting, Investigation and Handling of Cybersecurity Incidents for the Securities and Futures Sector, which took effect on 4 June 2021, provide that securities and futures institutions must report cybersecurity incidents immediately, and in the event of a severe incident the report shall be updated every 30 minutes. So, in addition to generally applicable reporting obligations, an organisation shall closely monitor and follow sector-specific regulations in order to comply with reporting obligations.

#### **WHAT ARE THE BIGGEST ISSUES THAT COMPANIES MUST ADDRESS FROM A PRIVACY PERSPECTIVE WHEN THEY SUFFER A DATA SECURITY INCIDENT?**

When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time. The biggest issues include, but are not limited to, assessment of severity and scope of damage; determination of whether to report the incident to regulators and affected individuals; technical rectification measures to control the incident to minimise damage; complete and swift internal review and investigation of the breach; coordination with outside legal, forensic, technical or public relations counsel to prepare for subsequent actions; cooperation with directives from regulators and the police (if necessary); responses to customer inquiries or complaints; and responses to media reports or coverage.

Any of these issues, if not handled properly, may easily morph into a situation that is out of control, especially in today's social media age. Such an incident is the true test of a company's response strategies, internal policies, management structure, designated staff and technical capabilities. The ultimate goal is to manage potential liabilities on all fronts, manage potential reputational damage, resume normal operation and prevent recurrence of similar incidents.

That said, out of these pressing issues, from a privacy protection perspective companies must concentrate resources to assess damage that may be caused to the privacy of affected individuals and take effective measures as a first priority to contain and control such damage while completing all legally required reporting and other obligations.

### **WHAT BEST PRACTICES ARE ORGANISATIONS WITHIN YOUR JURISDICTION FOLLOWING TO IMPROVE CYBERSECURITY PREPAREDNESS?**

Following in the footsteps of the GDPR, China has made tremendous legislative efforts in data and cybersecurity laws and regulations. Some high-profile pieces of legislation and investigation cases have conveyed strong messages to companies operating in China. We have seen many leading companies make good progress with regard to improving their cybersecurity preparedness.

First and foremost, the best practices are to comply with governing laws and regulations. Therefore, it is advisable to assess a company's actual compliance work against the laws and regulations and take measures to fix any gaps.

In addition to the mandatory laws and regulations, a company may need to comply with national and industry-specific cybersecurity standards, including some technical standards as guidelines for their cybersecurity work. Typical examples include the information security technology data security technology and cybersecurity technology series of national standards formulated by the National Information Security Standardization Technical Committee.

The Cybersecurity Law encourages companies to take security certifications. By going through the certification process, a company can evaluate its own practices against the certification standards and make changes accordingly to improve cybersecurity. Internationally recognised certifications, including ISO/IEC 27001, are being widely adopted by Chinese organisations as well. Further, the PIPL lists personal information protection certification by CAC-designated professional agencies (PIP Certification) as a recognised 'safeguard' for cross-border data transfer. The PIP Certification mechanism was officially implemented in November 2022, and as at December 2023, five organisations have obtained this certification, including fintech and e-commerce giants Alipay, Shein and JD.com.

In terms of implementation of cybersecurity measures, companies need to mobilise resources to cover different areas. For example, they need to upgrade their IT infrastructure to maintain a high degree of cybersecurity; employ sufficient qualified technical staff; draft and implement necessary internal policies, especially an incident response policy; adjust the governance structure by appointing a data protection officer or similar roles; and seek readily available legal, forensic, technical and public relations advice in both the event of an incident and in their daily operation.

If any incident has escalated to a certain degree, companies tend to form special task forces with in-house legal and technical staff and, if necessary, outside counsel as well, to address these incidents. It will help defuse the situation in a professional and efficient way before it gets out of control.

## **ARE THERE SPECIAL DATA SECURITY AND PRIVACY CONCERNS THAT BUSINESSES SHOULD CONSIDER WHEN THINKING ABOUT MOVING DATA TO A CLOUD HOSTING ENVIRONMENT?**

Cloud services are one of the fastest growing areas in China in recent years, and multiple new national and industrial standards have been introduced to provide technical specifications and best practice guidance for the service providers. There are many factors for a company to consider and evaluate before it makes a decision to move data to a cloud hosting environment. These factors include, but are not limited to, security, flexibility, expansion capability, performance, cost and legal compliance. If a company decides to go the cloud, the general recommendation is to assess the possibility of constructing the company's own private cloud system or to deploy a hybrid cloud, and only if both are unrealistic, consider the public cloud.

With respect to special data security and privacy concerns, a company should evaluate such concerns in a larger context to determine the most suitable cloud service. As public cloud services cover a huge volume of users and multiple business models, they are more vulnerable to hacking. Hardware sharing is common for the public cloud. This means competitors using the same cloud services may share the same server. Further, the public cloud may not always meet certain compliance requirements, such as local storage of data. In contrast, a private cloud allows a company to deploy appropriate security measures as it sees fit, which will offer a higher degree of security. It is comparatively easier to meet compliance requirements using a private cloud. But the cost for a private cloud is also higher than the public cloud. Therefore, a company must strike a balance between the competing values of relevant factors in choosing cloud services.

The main users of private-only cloud services are financial institutes in China. Companies with data security and privacy concerns tend to separate data into different categories based on the security grades. For example, a customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to balance various compliance requirements with cost concerns.

A company shall closely monitor sector-specific regulations and standards with respect to cloud deployment. For example, the Ministry of Industry and Information Technology (MIIT) published multiple recommendatory standards (non-binding) for the telecoms sector since mid-2021. The People's Bank of China also published three recommendatory standards regarding cloud computing for financial institutions in late 2020.

Subject to its business model, a company shall closely monitor data security and privacy laws and regulations. It shall design its core products or services from the beginning of its operation with a concept of categorised separation of data in accordance with applicable laws and regulations. This will prove more efficient and cost-effective for the company when it decides to go on the cloud later.

Further, cross-border transfer of data could be a key concern when considering cloud deployment. Pursuant to the relevant regulations, storing data overseas is deemed as a form of CBDT, hence companies will need to go through the Security Assessment, enter into the Standard Contract with their cloud solution providers or obtain the PIP Certification, if the cloud servers are located outside of China and the transfer cannot be exempted in accordance with the Provisions. In addition to generally applicable laws and regulations,

companies in certain sectors (eg, credit business agencies, insurance companies, medical institutions, ride-hailing service providers and smart cars) are also subject to sectoral data localisation requirements.

Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market. Therefore, users of cloud service providers with a foreign background need to consider the business model of the service provider and consider whether it will have any impact on the services requested.

## **HOW IS THE GOVERNMENT IN YOUR JURISDICTION ADDRESSING SERIOUS CYBERSECURITY THREATS AND CRIMINAL ACTIVITY?**

The Chinese government takes serious cybersecurity threats and criminal activity seriously.

The CAC is the main regulator with first-hand knowledge of market trends and cybersecurity threats through law enforcement activities, based on which it will lead the promulgation of new or amended regulations to address such concerns.

Owing to the rapid development of mobile technologies, CAC and other competent regulators such as the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS) and the State Administration of Market Regulation (SAMR) have focused their law enforcement efforts in regulating mobile applications in recent years. These regulators have the authority under the law to request application stores to suspend or remove download channels for illegal applications. In the meantime, other sectoral regulators have also initiated special campaigns over the past year to urge relevant market players to identify and rectify non-compliant practices, such as the former China Banking and Insurance Regulatory Commission's campaign against banks and insurance companies and the State Postal Administration's campaign targeting at delivery companies.

If any criminal offence leads are discovered during their investigation or review, these cases will be referred by the relevant regulators to the police to initiate criminal investigations. Individual citizens or entities, especially those victims of cybersecurity threats, are also encouraged to report crimes to the authorities, while providers of network products are legally obliged to report verified cybersecurity loopholes to the MIIT.

Law enforcement actions against cybersecurity threats are increasing. Based on professional database search results, over 14,000 administrative sanctions were issued against cybersecurity breaches in 2023. The top ranking violations include failure to perform cybersecurity obligations, engagement in activities harming cybersecurity and provision of assistance for activities harming cybersecurity. Civil lawsuits and public interest lawsuits against cybersecurity breaches are also increasing. According to statistics of the Supreme People's Procuratorate (SPP), over 6,000 public interest lawsuits for personal information protection were filed by procuratorates at various levels in 2023.

There are likely to be criminal liabilities for cybersecurity and data violations. According to China's Criminal Law, criminal penalties for computer hacking-related offences range from three- to five-year, or even longer, imprisonment sentences. For other crimes (eg, fraud, theft and embezzlement) conducted via cybersecurity breaches, penalties for the

same crimes (conducted in a traditional offline matter as set out in the Criminal Law) will also apply. In addition, the Law on Anti-Telecoms and Internet Fraud took effective on 1 December 2022. This new Law aims at preventing and combating relevant crimes by telecoms, finance and internet regulations. According to official statistics from the MPS, in 2023 Chinese police solved around 437,000 criminal cases involving telecoms and cyber fraud.

The Supreme People's Court and provincial High Courts regularly publish cybersecurity crime model cases to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to rule on cases. As cybersecurity crimes tend to involve a large number of victims, the police and procuratorates usually take priority in handling these crimes.

### **WHEN COMPANIES CONTEMPLATE M&A DEALS, HOW SHOULD THEY FACTOR RISKS ARISING FROM PRIVACY AND DATA SECURITY ISSUES INTO THEIR DECISIONS?**

The risk factors vary for different M&A deals. For asset or equity deals with high privacy and data security concerns (eg, purchase of software with heavy collection of user data or the equity of a hotel chain with large customer check-in data or equities of a manufacturer with a large number of employees worldwide, among many other examples) privacy and data security liabilities should be a key, if not a deal-breaking, factor.

There are several steps to follow to minimise potential risks. First, a proper legal and technical due diligence must be done by the buyer. This is especially important for foreign investors who are not necessarily familiar with the relevant data implications in the China market. Often this exercise should be done against not only the Chinese law, but also the relevant laws to all the jurisdictions involved (eg, the portfolio companies have a cross-border structure established for capital financing reasons, or the investors have limited partners from different jurisdictions), which may trigger, among other things, cross-border data transfer concerns. Note the due diligence findings may prove a no go, and if that is the case, of course, the earlier the finding is made, the better for both parties.

Second, subject to the due diligence findings, some rectification measures shall be taken either before signing, or as closing conditions or post-closing covenants (depending on circumstances). The buyer should consider requesting a reduction in, inter alia, the valuation of the target and escrow arrangement to hedge against potential liabilities. Certain representations and warranties should be customised with certain carve-outs to reflect the due diligence findings.

Third, subject to the magnitude of potential legal liabilities due to violations of privacy and data security, the buyer may insist on special compensation (which can be as severe as, for example, reversing the deal or down to the personal liabilities of the individual sellers) or offset of remaining payments (in the case of a payment schedule in several tranches with some payable after closing).

Fourth, the buyer should consider relevant insurance policies to cover liabilities for privacy and data security violations.

From the seller's perspective, it is important to shortlist credible buyer candidates. Once serious negotiations have commenced with selected buyers, the seller shall provide

full disclosure to the buyers under a satisfactory confidentiality agreement. Properly documented full disclosure is the right defence for any subsequent buyer claim after closing. Further, as a general rule in M&A deals, the seller should consider setting certain time limits to provide any compensation, including for privacy and data security violations. Needless to say, operating in a compliant way (especially navigating the dynamic Chinese data law) from day one is important for the seller.

## The Inside Track

### **WHEN CHOOSING A LAWYER TO HELP WITH CYBERSECURITY, WHAT ARE THE KEY ATTRIBUTES CLIENTS SHOULD LOOK FOR?**

Each law firm has its own focused practices. Clients should seek cybersecurity advice from lawyers who have a long-term track record of experience in navigating cybersecurity and data protection with a legal and a sectoral eye where relevant to the client. As cybersecurity often goes beyond national borders and, more importantly, nowadays data legislation from key economies globally is influencing data legislation in other key economies so heavily (especially the GDPR's impacts globally), lawyers with international practice and experience can offer more solid advice and input from a comparative perspective. Good lawyers are always on top of the latest legal developments. Last but not least, reputation or comments on lawyers generated from previous deals may also be key attributes clients should look for.

### **WHAT ISSUES IN YOUR JURISDICTION MAKE ADVISING ON CYBERSECURITY AND PRIVACY COMPLEX OR INTERESTING?**

There are multiple layers of laws and regulations on cybersecurity and privacy in China. Some have only recently been adopted and without sufficient implementation rules, some may be in the draft stage and the cybersecurity and privacy-related legal framework is evolving at an extremely fast pace. We anticipate that this trend will continue in the next couple of years. In addition, multiple regulators may be in charge of the supervision of the same issues from different perspectives. Therefore, a client needs expert advice to help correctly analyse their case and navigate in the complex legal and regulatory framework for cybersecurity and privacy compliance in China.

### **HOW IS THE PRIVACY LANDSCAPE CHANGING IN YOUR JURISDICTION?**

The tripartite safeguard for data regulation (ie, the Cybersecurity Law, the Data Security Law and the PIPL) are all in place. Lower-level implementation regulations and recommendatory national standards are being drafted or amended accordingly. Key regulators will finalise their internal guidelines on law enforcement where applicable. Regional regulations on data and privacy are also emerging. All of these changes will shape the privacy and data protection regime in China. Businesses, especially multinational business undertakings with a China presence or selling products or services to China, would need to review their privacy approach to comply with these changes. Regulators are bringing enforcement up to speed with this new wave of legislation.

## WHAT TYPES OF CYBERSECURITY INCIDENTS SHOULD COMPANIES BE PARTICULARLY AWARE OF IN YOUR JURISDICTION?

Business should be particularly aware of cybersecurity incidents that may cause massive data loss, paralyse service access in wide geographic areas, affect a significant number of users, involve sensitive personal information, involve data (regardless of it being personal or non-personal data) in key sectors, stir up social unrest or involve state secrets, public interest or national security concerns.



---

**Jingyuan Shi**  
**Yuchen Lai**

jingyuan.shi@simmons-simmons.com  
yuchen.lai@simmons-simmons.com

---

Simmons & Simmons

[Read more from this firm on Lexology](#)