ALM | LAW.COM

CORPORATE COUNSEL

Conducting Investigations and Discovery in China: What Companies Need to Consider in Preparing for New Policies

By John Davis and Gary GAO

March 26, 2025

The change in the U.S. administration promises to bring escalated tensions with China. In addition to increased tariffs, export controls and sanctions, we may, for example, expect the renewal of DOJ efforts such as the "China Initiative," targeting Chinese individuals and companies suspected of economic espionage and IP theft. Companies operating in China and those working with Chinese businesses and supply chains should anticipate an uptick in regulatory inquiries and requirements as well as in trade secrets litigations and other civil actions – each of which may demand extensive investigation of data and witnesses in China.

The risk and uncertainty involved in conducting such cross-border investigations will likely only increase. Chinese law and policy impose significant restrictions compounded by unfavorable logistical, technology, cultural, and security factors. Such restrictions often unavoidably conflict with U.S. and other countries' disclosure expectations.

With both U.S. and China-based companies increasingly caught in the crosshairs, it is crucial to plan now to respond effectively to these demands. Part 1 of this series of articles will provide an overview of factors involved in conducting a data investigation in China, including:

- key China sovereignty, data protection and data security requirements,
- unique risks involved in investigating and collecting information located in China, and
- best practices for mitigating risk, including practical tips and proactive steps to ease pain points and defensibly collect data.

Credit: Rawpixel.com/Adobe Stock

Part 2 of the series, in turn, will discuss bridging the compliance gap between U.S. expectations and the reality in China, including considerations in planning review and transfer of data outside of China for use in your proceeding, as well as strategies to manage the often-oppositional demands of Chinese and U.S. authorities and disclosure requirements.

China Data Protection, Data Security and Data Transfer Requirements

Conducting investigations and discovery in China requires navigation of its complex, broad, overlapping and opaque blocking statutes and data protection and security laws. As a threshold matter, companies must ask if their actions are covered by *The International Criminal Judicial Assistance Law* (ICJAL), which prohibits persons in China from providing evidence or assistance to foreign criminal authorities. Companies obligated to conduct internal investigations into potential wrongdoing, or to respond to civil allegations that overlap with criminal proceedings, must walk a careful line in fulfilling their obligations at home and abroad.

Assuming the ICJAL threshold is cleared, companies must still assess whether the type of information subject of investigation is restricted by China's additional laws governing data discovery and transfer. Key among these laws are the following – although, depending on the matter, there are a host of additional laws that may require consideration:

- *The Amended Law on Guarding State Secrets* ("SSL") bars the unauthorized transfer from China of "state secrets" the export of which could harm Chinese security or national interests in nearly any aspects of China's economy and government, or "work secrets" that could cause "adverse effects if leaked".
- *The Data Security Law* ("DSL") broadly restricts the export from China of "core" and "important" data that may cause harm to China's security. While regulation clarifies that certain companies may presume data is ***non***-important absent self-classification or appropriate notice to the contrary, wide gaps in understanding remain and companies may wish to continue to assess data for DSL compliance given the potential for retroactive categorization. DSL Article 36 also flatly forbids the unapproved disclosure of information in China to foreign judicial or law enforcement agencies.
- *The Personal Information Protection Law* restricts the processing and use of personal information ("PII") in China (and sometimes abroad). It is somewhat similar to the EU's GDPR, albeit with unclear U.S. litigation-compatible transfer mechanisms. Article 41 of the PIPL, too, prohibits the unapproved disclosure of PII to foreign authorities.
- *The Cybersecurity Law*, among other things, requires that certain companies keep much of their data in China, and submit to a "security assessment" before some PII and "important" data may be exported.

U.S. courts have found some of these broader restrictions (*e.g.*, DSL 36 and PIPL Art. 41) not to block civil discovery where information is exchanged between private litigants. *E.g., In re Valsartan, Losartan, and Irbesartan Products Liab. Litig.*, 2021 WL 6010575 at *10 (D.N.J. Dec. 20, 2021). However, it is not clear that the underlying reasoning would apply if the proceeding involved a government agency or arbitral tribunal or, indeed, if Chinese authorities would agree with such holdings. Nor is it likely that use of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters would provide a viable alternate path to discovery. Foreign courts and other authorities are not permitted to directly collect any evidence (including by deposing a party or witness) within the territory of the PRC, and the long delays and challenges to any use of this method has rendered it effectively non-functional.

Violation of the above laws carries the risk of harsh civil, administrative and criminal sanctions and collateral negative impacts. Chinese authorities have reportedly brought enforcement actions against Chinese companies in relevant contexts. *See Global Investigations Review, The Practitioner's Guide to Global Investigations Third Edition, China* (February 8, 2024) (discussing investigation of China Auto Logistics based on its conduct of an internal investigation involving employee data). While U.S. courts have questioned the actual risk of serious sanctions from violations (*e.g., In re DiDi Glob. Inc. Sec. Litig.,* No. 21-CV-5807 (LAK), 2025 WL 267893, at *4 (S.D.N.Y. Jan. 22, 2025), such skepticism may provide little comfort to those subject to PRC jurisdiction.

Unique Risks in Investigating and Collecting Information in China

Legal and Regulatory Risks

As may be evident from the above discussion, it can be difficult to tell what investigative conduct and information is restricted and in what circumstances. On their face, these laws are sufficiently

expansive and uncertain in scope and enforcement as to undermine the collection and use of the very data that is needed for a company's investigation, without prior approval of one or more Chinese government agencies. Yet the compliance process can be maddening, and seeking guidance or approvals in an investigation scenario carries its own risks in timing, process and outcome. Enforcement and rulemaking power is often sector-specific and distributed among multiple agencies with unclear and overlapping jurisdiction and evolving interpretation. Further, companies may be hesitant to seek approvals based on concerns of triggering further investigations and intervention at home.

Companies facing these risks are well advised to consult with experienced counsel to help understand these laws and assess whether the information at issue is likely subject to restriction, and under what circumstances. Counsel may also advise companies on approval mechanisms and options of seeking government guidance, and in designing and implementing compliant processes consistent with clients' disclosure obligations and objectives.

Practical Challenges

Equally daunting in cross-border matters are practical challenges involved in speaking to witnesses and defensibly collecting and assessing reliable information in China:

- *Siloed, under resourced and inexperienced teams*. Chinese companies and branch offices often have small legal departments with little or no experience in international litigations or investigations. They may also lack the internal infrastructure and experienced technical personnel to assist with compliant and defensible investigations.
- *Difficulties in obtaining cooperation*. Investigations may trigger distrust and obstruction among employees, business partners, third-party data managers, and witnesses. To take a common example, a request to inspect employee personal devices for business communications may be met by insistence on an overly formal process or the response that the phone recently became unavailable. Similar barriers may pop up at any step of an investigation, from gaining access to company databases and witnesses to obtaining needed documentation from suppliers.
- *Technical challenges related to incompatible and bespoke technologies*: To a far greater degree than U.S. businesses, technology used by Chinese companies tends not to be friendly to U.S.-style discovery (*e.g.*, the preservation of metadata, bulk downloads, etc.). This poses challenges in using standard forensic and e-discovery tools and processes to search and harvest data, and requires additional time, workarounds, explanation and costs.
- *Inconsistent recordkeeping*: Records demanded by U.S. authorities are not necessarily those routinely kept by Chinese companies. For example, in supply chain investigations, there may be incomplete records of contractors and upstream providers and limited ways of getting them from third parties – who want little to do with the investigation.
- *Limitations on investigative autonomy:* Investigators often face restrictions on their movement and actions in China. Further, the threat of "whistleblowers" and the risk that they and their companies' own actions may be investigated is ever-present.

Best Practices to Mitigate Data Risk in Investigations

Practical Tips and Steps

Still, all is not lost. Companies at risk of cross-border investigations and litigation can take several proactive steps to ease pain points and abet a smoother process:

- *Pre-Investigation Planning:* Companies should consider the following steps: (a) conduct a thorough risk assessment to identify potential legal and regulatory issues, and competent authorities; (b) establish local teams, including legal, audit, and compliance, with clear protocols for compliant data preservation, collection, storage, and transfer; (c) identify alternate data sources outside of China where possible, (d) map and risk rate key data sets to expedite handling, and (e) train and educate executives and employees on the investigative process as well as employee conduct, whistleblower and data policies (such as data use and handling, confidentiality and BYOD policies).
- *Robust data tracking, categorization and governance policies.* Determine where company data is kept, how it was generated and by whom, its

content and risk, its accessibility, and employees' consent to its processing and use. In particular, set clear expectations about employee personal device and WeChat use, and the company's right to access devices and accounts used for business. And once collected, ensure that cross-border transfers are first vetted by knowledgeable legal counsel.

- *Experienced U.S. and local counsel and consultants.* Effective coordination of a U.S.-oriented investigation requires U.S. counsel experienced in managing the unique demands of cross-border matters. In many instances, moreover, such projects can be effectively impossible without strong local counsel and consultants who have relationships with regulators, know the guardrails and are willing to take risks based on experience. Local counsel commonly fill in gaps in internal legal departments, interact directly with witnesses and stakeholders, coordinate with investigators, translate and explain information requests, and otherwise act where U.S. counsel cannot. Similarly, in any significant data investigation, experienced e-discovery providers and consultants with local operations may be required to troubleshoot technology disconnects and to help with in-country data and review work before it may be accessed in the U.S.
- *Invest in additional resources to collect and validate information.* Use secure and compliant technology solutions for data collection and transfer. Check and double check the process; consider sampling data to ensure completeness and defensibility; put in place clear QC processes; and document the endeavor. Far better to spend time on the front end to mitigate data integrity, completeness and falsification risks than having to answer questions about anomalies and gaps when it comes time for disclosure.
- *Educate, but allow time for re-do's.* It is not unusual to have to expand or repeat collections that were incomplete or not conducted to U.S. requirements. Make sure data preservation is done early so that it is available for follow-up inspection, and that company actors understand the vital importance of such steps. Local counsel, in particular, may be helpful in this education process. Then, when collecting data, gain consents, follow up, confirm and consider escalation points to clear blocks on data flow.

Conclusion

As U.S.-China relations evolve, companies are well advised to prepare for increased governmental scrutiny and civil actions. By understanding key legal requirements, investing in and building compliance and response teams and processes, educating employees, and adopting best practices, companies can better navigate the complexities of investigations and discovery in China, and weather the coming storm.

Companies with operations and data in China should begin planning now to ensure they are well-positioned to respond to future demands and protect their interests in this challenging environment.

John Davis *is a member of Crowell & Moring's Litigation and Investigations Groups in New York, where he Co-Chairs its E-Discovery and Information Management Practice Group. He can be reached at jdavis@crowell.com. John has extensive experience as in-house and outside counsel conducting cross-border investigations, leading responses to governmental inquiries, representing companies in complex litigations, advising companies on data risk, and managing discovery projects and groups. John is an award-winning author and frequent lecturer on investigations, AI and information law issues.* ***Gary GAO (Jun GAO)*** *is a Partner at the Zhong Lun Law Firm in Shanghai, where he Co-Chairs the Compliance & Regulatory Department. He can be reached a gaojun@zhonglun.com. Gary is a skilled litigator with near 30 years experience in disputes, arbitration, mediation and negotiation, including domestic and cross border matters. In addition, Gary has served as an arbitrator in leading arbitration institutions, e.g., ICC, SIAC, HKIAC and etc. Gary further has rich work experience in compliance & regulatory including investigation, criminal issue, comprehensive compliance system, cyber security and data compliance, crisis issues and firewall program design and implementation.*